Data Protection and Information Governance

Policy and Framework

Document Owner	Benjamin Watts Tel: 03000 416814
Version	April 2025
Approved	01/04/25
Review	April 2026

What is it for?

This is a consolidation of KCC's former Data Protection and Information Governance policies, to make it easier for all to find out and understand what we need to do and how to do it.

Who is it for?

This guidance is aimed at all members of staff at KCC who are working with and around information that will interact with Information Governance Legislation

How to use it

Use the table of contents below to find the topic(s) that you need to learn more about - you can press control and click on a heading to be taken directly to the page you require

Foreword

This is a consolidation of KCC's former Data Protection and Information Governance policies, to make it easier to find out and understand what we all need to do and how to do it.

Data Protection and Information Governance are part of everything we do as a public authority; we handle personal information every day and have a duty to do everything we can to keep it safe and process it appropriately.

Protecting the confidentiality and integrity of personal information is critical.

In the UK, the Data Protection Act 2018 (DPA) and the United Kingdom General Data Protection Regulation (UK GDPR) is the law that protects personal privacy and upholds individuals' (sometimes referred to as 'data subjects') rights. It applies to anyone who handles or has access to people's personal data in the UK.

Information Governance is a term that describes the strategy and framework an organisation has in place to explore and evaluate how they work with information. For KCC this includes how we comply with data protection legislation, the Freedom of Information Act (FOIa), the Environmental Information Regulations (EIR), the Privacy and Electronic Communications Regulations (PECR) and more.

It is important that all staff understand what this means in practice when working at KCC, what our roles and responsibilities are and how this should affect our decision making; we must all make informed judgements about how information is gathered, used and ultimately deleted.

KCC collects and uses personal information about people for a number of specific lawful purposes as set out in detail in its privacy notice(s). These include carrying out its business and fulfilling its statutory obligations e.g. managing and planning services. Personal information is held on past, current and prospective customers/service users, employees, suppliers and others with whom we communicate.

This document sets out KCC's over-arching corporate principles for ensuring good data protection and information governance, assuring its legal and regulatory compliance. It is important that all staff have a general understanding of the law, particularly how it affects the decisions we make on how information is gathered, used and ultimately disposed of.

IG Library

(Ctrl + Click on each subject to learn more about it)

What is Personal Data?

'Personal data' is any information that relates to an identified or identifiable living individual who can be recognised directly or indirectly from the information. This means the information could be clearly identifying an individual, or it could mean that there are only snippets of information but someone with access to it and the means to identify it, could link it back to an individual.

The information referred to includes factors about a person that are specific to their physical, physiological, genetic, mental, economic, cultural or social identity. This includes any expression of opinion about an individual and intentions towards an individual. Under the UK GDPR, personal information includes an identifier such as a name, an identification number, location data or an online identifier.

In short: Can a living individual person be identified from the information in question? Or could the right person with the means to do so identify an individual from a snippet of information? If so, then it is personal data.

We must keep in mind that correct and lawful treatment of personal information will maintain confidence in KCC and that protecting the confidentiality and integrity of personal information is critical.

Special Categories of Personal Data

Often referred to as 'special category data', this is information about individuals that by its very nature is more sensitive and requires more safeguarding.

The UK GDPR defines special category data as:

- personal data revealing racial or ethnic origin.

- personal data revealing political opinions.
- personal data revealing religious or philosophical beliefs.
- personal data revealing trade union membership.
- genetic data.
- biometric data (where used for identification purposes).
- data concerning health.
- data concerning a person's sex life; and
- data concerning a person's sexual orientation.

This does not include personal data about criminal allegations, proceedings or convictions, as separate rules apply.

To lawfully process special category data, you must identify both a lawful basis under Article 6 of the UK GDPR and a separate condition for processing under Article 9. These do not have to be linked.

Storage and retention of personal information

Personal information will be kept securely in accordance with KCC's policies and data protection obligations.

Personal information should only be stored in appropriate locations depending on business need and purposes; this means that information should not be routinely kept in external sources where it does not belong, such as applications used for collaboration, as it places the data at risk.

An example of this would be creating a copy of information from a customer system and then keeping it in an email folder.

Personal information must not be retained for any longer than necessary. The length of time personal information should be retained will depend upon the circumstances, including the reasons why personal information was obtained. Staff should adhere to KCC's Records Management Policy with reference to its Retention Schedule.

Personal information that is no longer required will be deleted permanently from KCC's information systems and any hard copies will be destroyed securely.

IG Library

Criminal Records Information

Where criminal offence information relating to:

- convictions,
- offences or related security measures (including personal information relating to the alleged commission of offences by an individual or

proceedings for an offence committed or alleged to have been committed, including sentencing)

is processed, a lawful condition for processing that information must also be identified and documented as set out in Schedule 1 of the Data Protection Act 2018.

These include:

- consent
- protecting a person's vital interests
- personal data in the public domain
- legal claims
- judicial acts
- any of the conditions listed under substantial public interest
- insurance.

A policy document must also be in place and retained, and a record of processing kept, as you would for special category personal information.

IG Library

Principles of Data Protection

If you would prefer to watch a short video that takes you through each of the principles in turn CTRL Click Principles of Data Protection

The principles set out in the UK GDPR must be adhered to when processing personal data. These principles should inform how we approach the work we undertake at KCC and should be applied to everything that we are doing with information.

Personal data must be processed lawfully, fairly and in a transparent manner ('**lawfulness, fairness and transparency'**).

This means making sure that we have a lawful reason to carry out the processing before we get started, then making sure that we do so in a fair way, alongside communicating with data subjects to explain what we are doing, why and how via a privacy notice.

Personal data shall be collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes ('**purpose limitation'**).

This means that we must only collect information for specific reasons and must use that information for the reason(s) we said we would when we requested it from the

data subject, unless the data subject has been informed of the new purposes, and they have consented where necessary.

Personal data shall be adequate, relevant and limited to what is necessary in relation to the purpose(s) for which they are processed ('**data minimisation'**). Staff may only process personal information when their role requires it.

This means that we should only ever collect and process the minimum amount of information that we actually need for what we are trying to achieve.

Personal data shall be accurate and where necessary kept up to date and every reasonable step must be taken to ensure that personal data that are inaccurate are erased or rectified without delay ('**accuracy'**).

This means that we have a responsibility to keep information as accurate as possible and take steps to update it when we find that it is not right.

Personal data shall be kept in a form which permits identification of data subjects for no longer than is necessary for the purpose(s) for which the personal data is processed ('**storage limitation'**)

This means that we should not keep information for longer than we need it for, in line with the retention schedule and what we have told data subjects.

Appropriate technical and organisational measures shall be taken to safeguard the rights and freedoms of the data subject and to ensure that personal data are processed in a manner that ensures appropriate security and protects against unauthorised or unlawful processing and against accidental loss or destruction of, or damage ('**integrity and confidentiality**')

Also known as the security principle, this means that we should make sure that measures are in place to protect information that is entrusted to us – both physically and electronically.

The accountability principle requires you to take responsibility for what you do with personal data and how you comply with the other principles. You must have appropriate measures and records in place to be able to demonstrate your compliance. ('**accountability**')

This means that we must take responsibility for what we are doing with personal data and demonstrate our compliance through our governance, processes, policies, and procedures. Data Protection Impact Assessments are a great tool to demonstrate compliance.

You can also use this table for an 'at a glance' guide to the principles:

Lawfulness, fairness and transparency	Ensure that there is a lawful basis to process the data then be open and honest with the data subject about what you are doing, why and how
Purpose limitation	Use the data only how you said you would
Data minimisation	Only collect the data you actually need
Accuracy	Keep data accurate and correct it if you find that it isn't
Storage limitation	Store it and destroy it appropriately
Integrity and confidentiality (security)	Make sure that appropriate measures are in place to keep information safe
Accountability	Take responsibility for our actions and carry out the appropriate governance

IG Library

Key Roles and Responsibilities

Information Governance (IG) is about having effective structures and policies in place to ensure legal and regulatory compliance, and the effective management of information risk. KCC is committed to ensuring that employees are aware of key roles and assigned responsibilities for Information Governance.

This framework sets out Kent County Council's (KCC) arrangements for ensuring personal information is handled securely and effectively, and in compliance with its legal and regulatory obligations.

KCC's aims are to:

- comply with data protection, freedom of information and related legislation
- respect individual's rights to privacy and confidentiality
- appropriately protect and secure information
- maintain accurate records
- use information to improve efficiency and enhance service delivery

This is achieved by:

- management accountability through designated roles and responsibilities outlined in this document
- a comprehensive policy framework supported, where appropriate, by strategies and improvement plans
- the Cross-Directorate Information Governance Group and Corporate Information Governance Group, providing support to KCC's Senior Information Risk Owner and DPO, to promote good information governance in accordance with their terms of reference
- Information Asset Owners (IAOs) ensuring that information risks are appropriately controlled within their service areas

- comprehensive guidance, training and support to managers and employees.

Please see the headings below for specific areas or go straight to the IG Framework structure chart.

Data Protection Officer

The General Counsel Benjamin Watts is the Data Protection Officer (DPO) and is responsible for informing and advising KCC and its staff on data protection obligations, and for monitoring compliance with those obligations and its policies. If you have any questions or comments about:

- the content of this document
- the lawful basis for processing personal information
- drafting privacy notices
- dealing with any rights exercised by an individual
- conducting a DPIA or planning any activities involving automated decision making
- sharing personal information

or if you need further guidance or believe that this policy is not being complied with you should contact the DPO via the DPO Support Team dpo@kent.gov.uk

Head of Risk and Delivery Assurance

The Head of Risk and Delivery Assurance is responsible for maintaining the Corporate Risk Register on behalf of the Corporate Management Team and Cabinet, ensuring that risks to KCC's strategic objectives are identified, assessed, and regularly reviewed. This includes strategic information risks identified by the Senior Information Risk Owner.

Senior Information Risk Owner

The Director of Strategy, Policy, Relationships and Corporate Assurance, David Whittle, is the Senior Information Risk Owner (SIRO). The SIRO understands KCC's strategic aims and how these may be impacted by information risks.

Responsibilities include:

- KCC's compliance with data protection, freedom of information and related legislation and records management.
- corporate information governance, assurance, policies and standards
- corporate information risk management
- ensuring KCC's information assets are identified, appropriately owned and documented and that associated risks understood and controlled.
- ensuring that the appropriate resources are available to implement and monitor the Records Management Guidance

Caldicott Guardian

The Caldicott Guardian is the senior person responsible for protecting the confidentiality of service-user information and enabling appropriate information-sharing.

The Guardian provides advice and will support decision making, if you are not sure whether you should share information, contact the Caldicott Guardian support officer in your Directorate; they will talk through the circumstances and help you to come to the right conclusion.

Requests for Caldicott Guardian consultation on DPIAs can be sent directly to Richard Smith, Corporate Director for ASCH, via email

Further information about this function can be found later in this document in the section Confidential Information and the Caldicott Guardian and on the dedicated KNet page.

Information Resilience and Transparency Team

The Information Resilience and Transparency Team's primary objective is to facilitate KCC's compliance with Information Governance legislation.

Information Asset Owners (IAOs)

KCC's IAOs are responsible for ensuring information assets within their services are properly recorded, documented and that associated risks are effectively managed. This includes approving Data Protection Impact Assessments (DPIAs) prior to submission to the DPO and signing off DPIAs (approving high risk processing and any further mitigation of risks identified by the DPO as necessary) once advice is obtained from the DPO.

IG Leads

Information Governance Leads are responsible for providing advice and guidance to their Directorate on a range of IG topics. All Divisional/Directorate Leads for Information Governance (listed on KNET) should conduct regular reviews of the personal information KCC processes within their division and update documentation accordingly. This may include:

- carrying out information audits to find out what personal information is held.
- talking to staff about processing activities
- producing and updating data mapping
- reviewing DPIAs
- reviewing KCC policies, procedures, contracts, and agreements to address retention, security and data sharing.

Please note that IG Leads cannot provide legal advice on contracts and agreements.

Chief Information Officer (CIO)

The Director of Infrastructure is also KCC's CIO who provides vision and leadership in the development and implementation of KCC's technology and commissioning strategy. The CIO understands how KCC's strategic aims may be impacted by technology and information system risks and ensures these are managed effectively.

Responsibilities include:

- maintaining records of KCC's information systems (managed on behalf of the CIO by the Business Services Centre).
- Corporate Information Security, Technology Risk and Compliance
- Technology Strategy and Commissioning

Records Manager

The Records Manager is responsible for developing KCC's information life cycle and records management policies, standards and practice. Providing advice and training to business managers, the Records Manager maintains the Corporate Information Asset Register for the SIRO and KCC's Information Asset Owners together with maintaining records inventories and retention. KCC's Records Manager is Elizabeth Barber.

Corporate Information Governance Group (CIGG)

The principal purpose of this group is to support the Senior Information Risk Owner (SIRO) and the DPO on information assurance, risk and compliance matters in accordance with its terms of reference. The group meets quarterly and is made up of representatives from across KCC's services.

The Group is jointly chaired by the SIRO and the DPO and is accountable to the Corporate Management Team.

Information Governance Cross Directorate Working Group (IGXDWG)

The principal purpose of the Information Governance Cross-Directorate Working Group is to support the Data Protection Officer and the Senior Information Risk Owner to monitor the council's compliance with information governance, to identify areas of good practice and areas for development, to review progress against the action plan and to report to the Corporate Information Governance Group.

CTRL Click Terms of Reference to download the terms of reference for both groups.

Kent & Medway Information Partnership

The Kent and Medway Information Partnership is a local public service partnership and not a council function. Kent County Council is a member of the partnership and bound by its terms of reference.

Established to improve information governance policy and practice, the Partnership offers networking and knowledge-sharing for practitioners. Local implications of

national developments and changes are considered and where appropriate joint strategies agreed.

This Partnership owns the Kent and Medway Information Sharing Agreement (KMISA), a high-level multi-agency protocol that provides a framework and templates for multi-agency information sharing. It is important to note that the agreement does not in itself provide a lawful basis for sharing information, rather it sets out a framework of expectations for how data should be handled in instances where it is appropriate to share between partner organisations.

CTRL Click Kent and Medway Information Partnership to find out more information.

Kent County Council

Kent County Council is a data controller, registered with the Information Commissioner's Office. As a data controller, KCC must ensure while processing personal data, all the requirements set out in the DPA 18, and UK GDPR are complied with.

Individual responsibilities

Staff may have access to the personal information of other members of staff, suppliers, clients or the public in the course of their employment or engagement. Where this is the case, staff must help KCC meet its data protection obligations to those individuals.

If staff have access to personal information, they must:

- only access the personal information that they have authority to access, and only for authorised purposes.
- only allow other KCC staff to access personal information if they have appropriate authorisation.
- only allow individuals who are not KCC staff to access personal information if they have specific authority to do so.
- keep personal information secure (e.g. by complying with the Secure Email Policy, with rules on access to premises, computer access, password protection and secure file storage and destruction in accordance with KCC's Information Security and Records Management Policies).
- not remove personal information, or devices containing personal information (or which can be used to access it) from the council's premises, unless appropriate security measures are in place (pseudonymisation, encryption or password protection, or a secure bag for physical records) to secure the information and the device
- not store personal information on local drives or on personal devices that are used for work purposes under the Bring Your Own Device (BYOD) scheme
- and comply with KCC's ICT Acceptable Use Policy

KCC promotes good practice through regular and targeted communications to staff via their managers, KNet and KMail.

As a KCC employee, you play an important role in ensuring good information governance. To do this, you are expected to:

a) protect personal and confidential information.
b) understand and comply with information governance and data protection policies and procedures.
c) act in accordance with training, guidance and verbal instructions
d) IMMEDIATELY (and at the latest within 1 hour) report any information security incidents to their line manager and ICT (where appropriate), try and retrieve any lost data or equipment and follow the Data Breach guidance in the event of any loss of data.

Team Responsibilities

- Managers and supervisors are responsible for ensuring employees (including temporary staff) complete mandatory information governance and data protection training on induction and subsequently as required, and for ensuring completion is recorded.
- Managers and supervisors are expected to have a working knowledge of information governance policies and an understanding of the legislative framework applicable to their service or team activities and operations. They must understand their responsibilities as outlined in these policies.
- Managers and Team Leaders are responsible for documenting procedures and developing effective practice within their service areas, to include integrating core privacy considerations into existing project management and risk management methodologies and policies.
- KCC investigates information security incidents and aims to learn lessons as the basis for continuous improvement. All staff must be aware of KCC's policies around Data Breaches.
- All staff must ensure that they access and use information only as authorised by KCC and for professional reasons as required by the Kent Code, the ICT Acceptable Use Policy and this Policy. Inappropriate or unauthorised use or disclosure of information; or unlawful obtaining, disclosing or retaining of personal data without the consent of KCC may lead to offences under the Computer Misuse Act 1990 and/or the Data Protection Act 2018.

Specific Roles in Data Sharing

Directors are accountable to their Corporate Directors (Information Asset Owners) for their services' adherence to policy and ensuring accurate records of sharing activities are maintained.

Directors whose services share significant volumes of personal data may choose to nominate Lead Officers.

Lead Officers are responsible for maintaining the quality and recording of information sharing arrangements within their services.

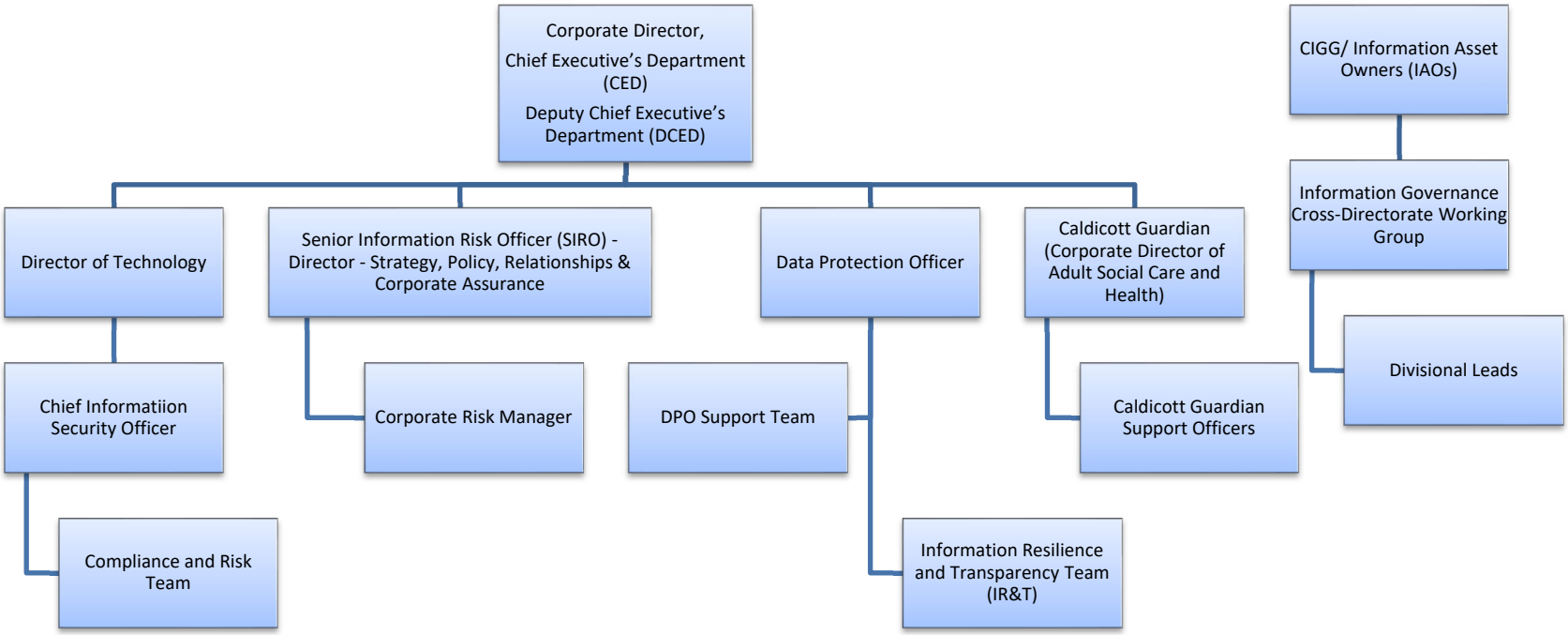
Lead Officers are those named on information sharing documentation as the responsible officer for a particular sharing arrangement.

Lead Officers are responsible for:

- corporate visibility and reporting of information sharing within their services
- providing a point of contact for audit and enquiries
- ensuring arrangements are reviewed within their stated periods
- notifying relevant officers when a new arrangement is put in place or where an existing arrangement is terminated or changed.

IG Library

Information governance management structure



Confidential Information and the Caldicott Guardian

Confidentiality is an important legal and ethical duty established in the common law (derived from Court judgments). It is the principle that information given or obtained in confidence should not be used or disclosed further (including internally) except in certain circumstances e.g. the individual consents, the disclosure is required by law, or by a court order, or it is exceptionally justifiable in the public interest.

Any use of confidential information relating to an individual's health or adult social care other than for direct care and support must have a sound legal basis. It cannot be shared, even internally, without written prior approval from KCC's Caldicott Guardian.

a) Requests for confidential information should be made to the data owner in the first instance.
b) The data owners' Caldicott Guardian Support Officer (CGSO) must apply the Caldicott Principles and may request clarifications or set conditions before making a recommendation to the Caldicott Guardian.
c) The Caldicott Guardian will review the recommendations and make a decision, or the CGSO will decide on the CG's behalf.

An effective Caldicott function ensures that confidential information relating to an individual's health or adult social care is handled and shared under strict controls. From April 2018 the NHS's Data Security and Protection Toolkit has formed part of a new framework for assuring that health and social care organisations are implementing the ten data security standards recommended by the former National Data Guardian Dame Fiona Caldicott. KCC is committed to compliance with the toolkit and implementing the security standards.

KCC is required to have regard to the Code of Practice on Confidential Information issued under section 263(1) of the Health and Social Care Act 2012. Confidential patient information may be disclosed in very limited circumstances:

a) the patient/social care client consents, whether implicitly or explicitly for the sake of their own care or for local clinical audit, or explicitly for other purposes
b) the patient/social care client has given their explicit consent to disclosure for other purposes
c) the disclosure is of overall benefit to a patient who lacks the capacity to consent
d) the disclosure is required by law, or the disclosure is permitted or has been approved under a statutory process that sets aside the common law duty of confidentiality

e) the disclosure can be justified in the public interest

When disclosing information about a patient you must:

a) use anonymised information if it is practicable to do so and if it will serve the purpose
b) be satisfied that the patient:
    i. has ready access to information explaining how their personal information will be used for their own care or local clinical audit and that they have a right to object
    ii. has not objected
c) get the patient's explicit consent if identifiable information is to be disclosed for purposes other than their own care or local clinical audit, unless the disclosure is required by law or can be justified in the public interest
d) keep disclosures to the minimum necessary for the purpose
e) follow all relevant legal requirements, including the common law and data protection law.

You must keep a record of your decision and actions. This will ordinarily be kept by the Caldicott Guardian. You should tell patients about disclosures you make that they would not reasonably expect, or check they have received information about such disclosures, unless that is not practicable or would undermine the purpose of the disclosure - e.g. by prejudicing the prevention, detection or prosecution of serious crime.

The Health and Social Care (Safety and Quality) Act 2015 (England) places a duty on providers and commissioners of health and social care in England to share information when it is considered likely to facilitate the provision of health or social care to an individual and when it is in the individual's best interests. The duty will not apply where an individual objects (or would be likely to object), or where the information relates to the provision of care by an anonymous provider or where the duty cannot be reasonably complied with for other reasons. The duty does not override duties under the common law or Data Protection Act 2018.

Section 251 of the NHS Act 2006 allows the Secretary of State for Health to make regulations to set aside the common law duty of confidentiality for defined medical purposes. In practice, this means the person responsible for the information can disclose confidential patient information without consent to an applicant without being in breach of the common law duty of confidentiality, if the requirements of the regulations are met. The person responsible for the information must still comply with other relevant legal obligations such as the Data Protection Act 2018 and the Human Rights Act 1998.

The regulations that enable this power are called the Health Service (Control of Patient Information) Regulations 2002. Any references to 'section 251 support or approval' refer to approval given under the authority of the regulations. These

powers can only be used where it is not practical to obtain consent and anonymised information cannot be used, having regard to the cost and available technology. They cannot be used to permit information to be disclosed solely or principally for the direct care of individual patients e.g.

- Regulation 3: disclosure by and to bodies listed in paragraph 3 when processing is intended to diagnose, control or prevent, or recognise trends in, communicable diseases and other risks to public health. (see footnote)
- Regulation 5: disclosure for a range of purposes including 'preventative medicine, medical diagnosis, medical research, the provision of care and treatment and the management of health and social care services'. An application needs to be submitted to the Confidentiality Advisory Group (CAG) of the Health Research Authority (HRA). The CAG give advice to the relevant decision maker, which is currently the HRA for research applications and the Secretary of State for Health for non-research application.

The National Data Opt-Out Policy

The National Data opt-out was introduced to give patients (which includes social care users) a choice on how their confidential patient information is used for purposes beyond their individual care. The opt-out applies to special category data as it includes information about a patient's health or social care and/or treatment that has been collected as part of the care provided. Patients can set or change their choice with NHS Digital online. The opt-out is recorded against the patient's NHS Number in a repository held by the NHS.

This Policy requires all health and social care organisations (including organisations under contract with local authorities) to comply. In accordance with the patient's wishes and national data opt-out policy, as a health and care organisation located in England, KCC is required to apply national data opt-outs when applicable to a use or disclosure of confidential patient information for purposes other than the patient's care or treatment.

NHS Digital offer a service which allows organisations to submit a list of NHS numbers to check if data subjects have registered their preference with NHS Digital's national repository so that their confidential patient information cannot be used for secondary care purposes (purposes other than direct or 'primary' clinical care). The resulting 'cleaned' list is applied to disclosures of confidential patient information in accordance with the National Policy.

Some disclosures do not require the application of the national data opt-out because:

- the data being disclosed is anonymised in line with the ICO's Code of Practice on Anonymisation, or
- consent has been obtained from the individual for their data to be used for the specific purpose, or

- there is a mandatory legal requirement that sets aside the common law duty of confidentiality, or the information is required by a court order, or
- there is an overriding public interest for the data to be shared, or
- the confidential patient information is only used for direct individual care, or
- the data disclosure is made under Regulation 3 of the Control of Patient Information Regulations 2002 (for communicable diseases and other risks to public health) and is exempt from the National Data Opt-Out.

This policy does not apply to children's social care or education services, but child health services provided through organisations regulated by the Care Quality Commission do remain in scope.

Please visit ASCH Internal NDOOP for further information.

IG Library

Lawful Basis for Processing Personal Information

Before any processing activity starts for the first time, the purpose(s) for the processing activity and the most appropriate lawful basis (or bases) for that processing must be selected and recorded.

KCC anticipates that most of its processing will be necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller. These apply where KCC has a duty or power set out in legislation or statutory guidance. Where it is appropriate to rely on legitimate interests, for processing activities outside the scope of its tasks as a public authority (for example in relation to KCC's commercial interests), it will provide details of the balancing test carried out.

IMPORTANT: Staff must be satisfied that the processing is necessary for the purpose of the relevant lawful basis (and that there is no other reasonable way to achieve that purpose).

Under Article 6 of the UK GDPR, it must be determined whether:

- the data subject has given consent to the processing of his or her personal information for one or more specific purposes.
  This means that the data subject has specifically given consent for a processing activity.
- processing is necessary for the performance of a contract to which the data subject is party, or in order to take steps at the request of the data subject prior to entering into a contract.

This relates to contracts that are entered into with an individual, such as when they request for a service to be delivered.

- processing is necessary for compliance with a legal obligation to which KCC is subject.
  This relates to when a piece of legislation requires KCC to process data, such as employment information that must be shared with HMRC.
- processing is necessary in order to protect the vital interests of the data subject or of another natural person.
  This means that the processing is necessary to protect a life when the data subject cannot otherwise provide their consent.
- processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in KCC.
  This relates to when KCC is fulfilling its statutory duties and should be backed up with a point of legislation or statutory guidance requiring the processing to take place.
- processing is necessary for the purposes of the legitimate interests pursued by KCC or by a third party.
  This relates to when it can be assessed that there is a legitimate interest in processing an individual's information as they would reasonably expect it to happen. This basis is incompatible with 'public tasks' and cannot be relied upon when fulfilling statutory duties. You should also take care to ensure that the Privacy and Electronic Communications Regulations are complied with when considering relying on this basis for communicating with individuals.

The decision as to which lawful basis or bases applies must be documented, to demonstrate compliance with the data protection principles. Information must be provided about both the purpose(s) of the processing and the lawful basis for it in KCC's relevant privacy notice(s). Take care when determining the lawful basis that will be relied upon, the lawful basis should not be changed later without good reason, and consent cannot usually be swapped for a different basis.

Do you know what the lawful basis is for the processing your team undertakes? If not take a look at the suite of privacy notices on Kent.gov and find the relevant one for your work – it is important that we all understand this so that we can support our data subjects in understanding what we are doing and why.

IG Library

Consent

The UK GDPR sets a high standard for consent. It must be freely given, unambiguous and kept separate from other agreements or contracts. Data subjects must be easily able to withdraw consent to processing at any time and withdrawal

must be promptly honoured. Agreement must be indicated clearly, either by a statement or positive action to the processing.

Consent requires affirmative action, so silence, pre-ticked boxes or inactivity are not sufficient.

Consent may need to be refreshed if personal information is intended to be processed for a different and incompatible purpose which was not disclosed when the data subject first consented. If we have said we will use data for something and obtained consent, we can't then use the data for something else further down the line as the data subject is not aware and did not consent to that additional use.

If the individual has no real choice, feels compelled to consent or will endure negative consequences if they do not consent, then consent will not be valid. Consent will not be freely given if the data subject is unable to refuse or withdraw their consent without detriment.

Where explicit consent is required for processing special category personal information, evidence of consent will need to be captured and recorded so that KCC can demonstrate its compliance with the law.

It is important not to confuse consent sought for other purposes e.g. an ethical or common law requirement, with the Article 6(1)(a) consent lawful basis for processing under data protection legislation. The lawful basis for processing under data protection law as set out in the UK GDPR and the Data Protection Act 2018 may be something other than consent, with consent (permission) still sought for, for example, participation in research.

Staff should be aware that patient consent for treatment or to share healthcare records is not the same as the UK GDPR consent lawful basis.

In the healthcare sector, patient data is held under a duty of confidence. Healthcare providers generally operate on the basis of implied consent to use patient data for the purposes of direct care, without breaching confidentiality. Implied consent for direct care is industry practice in that context but this 'implied consent' in terms of duty of confidence is not the same as consent to process personal data in the context of a lawful basis under the UK GDPR. Any requirement to get consent to the medical treatment itself does not mean that there is a requirement to get UK GDPR consent to associated processing of personal data, and other lawful bases are likely to be more appropriate.

IG Library

Lawful Bases – Special Categories of Personal Data

Special Categories of Personal Data refers to information that by its very nature is more sensitive and requires additional safeguards.

Processing of this information is prohibited unless a lawful special condition is identified.

Under Article 9 of the UK GDPR, special category personal information will only be processed if there is a lawful basis for doing so as identified and one of the special conditions for processing special category personal information applies:

a) the individual has given explicit consent
   please see the information on consent above
b) the processing is necessary for the purposes of exercising KCC's or an individual's employment, social security or social protection law rights or obligations
   this is when KCC must process special categories of personal data for these purposes
c) the processing is necessary to protect the data subject's vital interests, and the data subject is physically or legally incapable of giving consent
   this is when we need to process the data to protect an individual's life when they are not otherwise able to consent.
d) the processing is carried out by a not-for-profit body with a political, philosophical, religious or trade union aim in relation to its members
   this basis is only likely to become relevant for KCC if we are involved with commissioning a service that specifically fits the description above.
e) the processing relates to personal data which are manifestly made public by the data subject
   this is when a data subject has themselves already made their information publicly available
f) the processing is necessary for the establishment, exercise or defence of legal claims or where courts are acting in their judicial capacity
   this is when we must process the information for matters relating to legal claims or casework for example
g) the processing is necessary for reasons of substantial public interest
   this is closely aligned to our public duties and would be relevant when we need to process data to satisfy a duty or some work that is in the public interest
h) the processing is necessary for purposes of preventative or occupational medicine, for the assessment of the working capacity of the employee, the

provision of social care and the management of social care systems or services
this is when we need to process data to provide health and social care services to a data subject

i) the processing is necessary for reasons of public interest in the area of public health
this basis relates specifically to processing data for the purposes of public health

j) the processing is necessary for archiving purposes in the public interest, or scientific and historical research purposes or statistical purposes (subject to appropriate safeguards).
this basis relates to the work we do in archiving and research

Schedule 1 of the Data Protection Act 2018 sets out further conditions and safeguards which must additionally be observed when processing special category data.

The additional conditions that the processing is necessary for include:

- performing obligations or exercising rights in connection with employment, social security or social protection law
- health or social care purposes (only under obligation of secrecy)
- reasons of public interest in the area of public health (and carried out by a health professional)
- archiving purposes, scientific or historical research purposes or statistical purposes in the public interest
- specific reasons of 'substantial public interest'

Those conditions can be explored in more detail via the Data Protection Act 2018 and guidance on the ICO's website relating to processing special category data. These requirements must be carefully considered when considering whether they provide a lawful gateway for processing special category data.

Read the Data Protection Act 2018 in full at the following link:
http://www.legislation.gov.uk/ukpga/2018/12/contents/enacted

Where KCC is relying on certain additional conditions in the Data Protection Act as outlined above - employment obligations, substantial public interest or criminal convictions - the following safeguards must also be in place:

- an appropriate policy document which explains: the procedure for complying with the UK GDPR Principles when relying on these additional conditions; and the retention and erasure of information processed under the additional conditions. (See KCC's Retention Schedule in relation to this)

- the policy document(s) must be retained for at least 6 months after processing has ended, regularly reviewed and updated and available to the ICO upon request
- a record must be maintained within the Record of Processing Activity (ROPA) of the processing of personal data in reliance on these conditions which specifies:

    a) the condition relied on

    b) how it satisfies Article 6 (lawful bases of processing) and

    c) whether personal data is retained and erased in accordance with KCC's Retention Schedule and if not, the reasons why.

  This will also be recorded in a Data Protection Impact Assessment (DPIA).

Where conditions rely on processing being demonstrably 'necessary' for a specific purpose, this means that processing must be more than just useful or habitual. It must be a targeted and proportionate way of achieving that purpose. The condition also does not apply if you can reasonably achieve the same purpose by some other less intrusive means – and in particular if you could do so by using non-special category data. The data minimisation principle should be considered carefully for all data but especially special category data.

Important: Special category personal information must not be processed until KCC is assured that the processing activity complies with the criteria above and the individual has been informed (by way of a privacy notice or otherwise) of the nature of the processing, the purposes for which it is being carried out and the legal basis for it.

IG Library

Privacy Notices

KCC will issue privacy notices as required, informing individuals about the personal information that it collects and holds and details of how individuals can expect their personal information to be used and for what purposes.

This forms a vital part of our compliance with the 'Lawful, Fairness and Transparency' principle of the UK GDPR, as it is how we tell data subjects what we are doing, why we are doing it, who we may share information with and crucially what our lawful basis is for doing so.

CTRL Click Privacy Notice Resource to view a video that explains the basics of how to approach writing a Privacy Notice.

KCC will explain in those notices the rights of individuals and will take appropriate measures to provide information in a concise, transparent, intelligible and easily accessible form, using clear and plain language. Sometimes it may be relevant and necessary to provide a privacy notice in alternative formats, such as 'easy read', braille or other languages. Staff seeking support in this area can contact the alternativeformats@kent.gov.uk mailbox.

When information is collected directly from individuals, including for HR or employment purposes, the individual shall be given all the information required by the UK GDPR including the identity of the data controller and the DPO, how and why KCC will use, process, disclose, protect and retain that personal information through a privacy notice (which must be presented when the data subject first provides the personal information).

When information is collected indirectly (for example from a third party or publicly available source) the individual must be provided with all the information required by the UK GDPR as soon as possible after collecting or receiving the personal information and no later than one month from that date. Data collected by a third party must also be obtained in accordance with the UK GDPR and used in a way that is consistent with the proposed use of the personal information set out in the privacy notice. Individuals will be informed about the way their personal information is used and who it may be shared with at the time it is collected.

For detailed guidance and the KCC template, please see the Privacy Notice Guidance.docx (sharepoint.com) on KNet.

IG Library

Data Breaches

This guidance applies to all KCC staff and volunteers and, through contractual arrangements with KCC, suppliers, partners, contractors, agents, consultants and commissioned services, in the course of functions carried out for or on behalf of KCC.

Members (elected Councillors) are bound by obligations under the Members' Code of Conduct but must also be aware of their corporate and personal responsibilities to understand the requirements of the UK GDPR and to act in response to any breaches in relation to personal data.

A personal data breach means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data transmitted, stored or otherwise processed. This means that a personal data breach is more than just losing personal data.

Prevention is always better than cure. Data security concerns may arise at any time and staff are encouraged to report any concerns they have to the Data Protection Officer (the DPO) or the Information Resilience and Transparency Team (IR&T). This helps KCC to capture risks as they emerge, protect information and KCC from data breaches, and keep processes up-to-date and effective.

Whilst instances of the loss of personal data are rare, the consequences to KCC's reputation and the potential impact on the individuals whose data is breached (whether they are service users or other employees) means that it is essential to take swift and appropriate action in the event of a data breach.

The Information Commissioner's Office (ICO) can impose significant fines on data controllers for serious contraventions of the UK GDPR. It can also serve an enforcement notice on data controllers if it considers positive steps are necessary to bring about compliance.

Personal data breaches may involve criminal or civil liability, or both, depending on the circumstances, and may include both individual and corporate responsibility.

A data breach may take many different forms:

- loss or theft of data or equipment on which personal information is stored
- unauthorised access to or use of personal information either by a member of staff or third party
- loss of data resulting from an equipment or systems (including hardware or software) failure
- human error, such as accidental deletion or alteration of data or emailing the wrong individual or pressing 'reply all' instead of 'reply'
- unforeseen circumstances, such as a fire or flood
- deliberate attacks on IT systems, such as hacking, viruses or phishing scams
- blagging offences where information is obtained by deceiving the organisation which holds it

The initial steps that should be taken to alert managers about an incident will vary depending on whether the incident involved a member of KCC staff, a supplier or commissioned service, a service user or member of the public or an elected Member.

Staff must inform their manager immediately if a data breach is discovered and make all reasonable efforts to recover any information. Staff and managers must have regard to this policy and their responsibility to report data breaches or suspected information security incidents.

Action to take on discovery of the breach

If an information breach has occurred or may occur, the officer or other person concerned should:

a. where possible, retrieve any lost equipment or papers
b. where theft or the loss of sensitive information which could risk the safety of others is involved, report the incident to the police with all relevant details
c. Notify their manager/a KCC member of staff as follows:
    i. Employees and contract workers should notify their line manager, or (if unavailable) the next senior manager.
    ii. Suppliers of Commissioned services (sometimes referred to as 'Data Processors') should inform their KCC contract manager.
    iii. Where a data breach is reported to the contact centre by a member of the public, the contact centre must inform IR&T, who will refer the incident to the relevant member of staff.
    iv. Elected members who identify a breach relating to their role within the council (not as a representative of their ward or political party) should initially contact the Head of Service or Corporate Director concerned.
d. Report the loss of any ICT equipment or an electronic security breach to the ICT Service Desk. Where the security breach or suspected security breach involves Justice Data or access to the CJSM, this must be reported to the CJSM Administrators immediately (via the CJSM Helpdesk).
e. Complete PART ONE of the data breach report form. The responses to the form will be shared with the relevant line manager.
f. An anonymous report can be submitted by a non-electronic method, e.g. internal post to the IR&T team or the DPO.

Staff should report incidents via this form: Data Breach Report Form

The form is in two parts. Part One notifies the Information Resilience and Transparency (IR&T) team of a suspected data breach and Part Two outlines the details of the investigation and the mitigating actions that have been put in place. The information submitted in Part One will be reviewed and the person responsible for investigating the breach contacted; this email will include a link to complete the second part of the form.

Following notification, the officer or other person should not take any further action in relation to the breach. In particular, they must not notify any affected individuals or regulators.

In the event of a suspected personal data or information security breach: DO NOT WAIT; ACT and REPORT ANY INCIDENTS IMMEDIATELY

Managing the Breach

Once the data breach form has been submitted a receipt acknowledging the data breach report form will be received. The breach will automatically be entered in the security incident log and the IR&T team will review and take appropriate steps to deal with the report in collaboration with the appropriate data breach owner.

If a breach is suspected to have taken place the following information will be required within the data breach report form to assess the seriousness of the breach.

a. What type of data is involved?
b. How sensitive is the data?
c. Who is affected by the breach, i.e. the categories and approximate number of data subjects involved?
d. The likely consequences of the breach on affected data subjects. E.g. what harm can come to those individuals, are there risks to physical safety or reputation, or financial loss?
e. Where data has been lost or stolen, are there any protections in place such as encryption or pseudonymisation?
f. What has happened to the data, e.g. if data has been stolen, could it be used for harmful purposes?
g. What could the data tell a third party about the data subject, e.g. could the loss of apparently trivial snippets of information help a determined fraudster build up a detailed picture of other people?
h. What are the likely or wider consequences of the personal data breach on KCC e.g. loss of reputation, loss of business, liability for fines, loss of public confidence?

The data breach owner will take immediate steps to establish whether a personal data breach has, in fact, occurred. If so, the data breach owner will take appropriate action to:

- Investigate and contain the data breach and (so far as reasonably practicable) recover, rectify or delete the data that has been lost, damaged or disclosed (subject to any requirements to preserve potential evidence)
- Identify how the breach occurred and take immediate steps to stop or minimise the further loss, destruction or unauthorised disclosure of personal data
- Notify appropriate parties of the breach and informing them what they must do (this could be finding lost equipment, isolating or closing part of the network or changing passwords)
- Fully assess the risk in terms of the potential adverse consequences for individuals: how serious are the consequences and how likely are they to happen?
- Take steps to prevent further breaches.

Notifying Other Parties

The data breach owner must discuss with the IR&T Team when they are considering whether to notify:

- The ICO
- Affected data subjects
- The Police or any other parties e.g. insurers or commercial partners

Ultimately the decision whether to notify lies with Corporate Directors in liaison with the DPO, particularly where the implications of the breach would seriously affect KCC's reputation. Failing to notify a breach when required to do so can result in a significant fine.

Notifying the Information Commissioner's Office (ICO)

KCC is required under the UK GDPR to notify the ICO when a personal data breach has occurred unless the personal data breach is unlikely to result in a risk to the rights and freedoms of data subjects. By this it means, but is not limited to:

- discrimination
- damage to reputation
- financial loss
- loss of confidentiality
- or any other significant economic or social disadvantage.

If it's likely that there will be a risk, then you must notify the ICO. If it's unlikely then you don't have to report it; however, you need to be able to justify this decision, so you should document it.

Where ICO notification is required, this shall be done without undue delay and, where feasible, not later than 72 hours after having become aware of it. Where the notification to the ICO is not made within 72 hours, it will be accompanied by reasons for the delay. The IR&T team will notify the ICO on behalf of Kent County Council and keep the DPO informed of the situation.

If the IR&T Team is unsure whether to report, the presumption should be to report.

Any notification to the ICO must:

a. Describe the nature of the personal data breach including, where possible, the categories and approximate number of data subjects concerned, and the categories and approximate number of personal data records concerned.
b. Communicate the name and contact details of the DPO or other contact who can provide information.
c. Describe the likely consequences of the personal data breach.

d. Describe the measures taken or proposed to be taken by KCC to address the personal data breach, including, where appropriate, measures to mitigate any possible adverse effects.

If all the information is not available within 72 hours this information may be provided in phases, provided the further information is provided to the ICO without undue further delay.

Notifying data subjects

Where the data breach is likely to result in a high risk to the rights and freedoms of data subjects, the data breach owner will notify the affected individual(s) without undue delay.

The risk exists when the breach leads to physical, material or non-material damage for the individuals whose data have been breached (this could include theft, fraud, financial loss, discrimination or damage to reputation). If the breach involves personal data that reveals any special category data, the damage should be considered likely to occur.

Any notification should detail the nature of the personal data breach and must include:

a. The name and contact details of the DPO or other contact point where more information can be obtained
b. The likely consequences of the personal data breach
c. The measures KCC has taken or intends to take to address the personal data breach, including, where appropriate, recommendations for mitigating potential adverse effects.

In some circumstances, service users are vulnerable adults and children and being informed of a security incident may be alarming. In these circumstances the IR&T Team and the data breach owner will consider appropriate communication strategies.

It may be important to point out at an early stage of a security incident (rather than a confirmed breach) that there is no indication that their personal security has been breached but the member of the public must remain vigilant and will be advised of any change in security status. If any of the information relates to personal finance details, then the individual should be advised to contact their bank or building society urgently and to monitor their bank/building society account(s).

Notifying the Police and other parties

The data breach owner will consider whether to contact the police for the purpose of containment and recovery. If it transpires that the breach arose from a criminal act perpetrated against or by a representative of KCC, the data breach owner will notify the police and/or relevant law enforcement.

The data breach owner will consider whether there are any legal or contractual requirements to notify any other parties, e.g. in compliance with a contract or a data sharing agreement.

Preventing future breaches

Once the personal data breach has been dealt with, in accordance with this plan, the data breach owner will:

- Establish what security measures were in place when the breach (or security incident) occurred,
- Assess whether technical or organisational measures can be implemented to prevent the breach happening again,
- Consider whether there is adequate staff awareness of security issues and address any gaps through training, tailored advice or capability,
- Consider the outcome of any investigations into the cause of the breach and whether action should be taken under KCC's disciplinary procedure,
- Consider whether it is necessary to update KCC's privacy risk assessments,
- Complete Part TWO of the Data Breach Report Form

Consequences of non-compliance

Failure to comply with this overarching policy and this specific guidance puts individuals and KCC at risk.

Failure to notify the DPO or IR&T of an actual or suspected personal data breach is a very serious issue.

A failure to comply with this policy by:

- **KCC employees:** may result in disciplinary action and may, in cases of Gross Misconduct (including negligence), result in termination of employment
- **KCC Members**: may be referred to the Standards Committee, which can recommend disciplinary measures to the Council
- **Third Parties**: (agents, contractors and consultants) engaged to carry out work for and on behalf of Kent County Council: may result in the termination of the contract and/or litigation.

Examples of Common Incidents

Example	Notify the ICO?	Notify the data subject	Notes
KCC stored a backup of an archive of personal data encrypted on a CD. The CD is	No	No	If the data are encrypted, backups of the data exist, and the unique key is not compromised, this may not be a

stolen during a break-in.			reportable breach.
KCC suffers a ransomware attack which results in all data being encrypted. No back-ups are available, and the data cannot be restored. On investigation, it becomes clear that the ransomware's only functionality was to encrypt the data and that there was no other malware present in the system.	Yes	Only the individuals affected are notified if there is a high risk and it is clear that others were not affected.	If, after further investigation, it is identified that more individuals are affected, an update to the ICO must be made and the additional step of notifying other individuals if there is a high risk to them.
Personal data of 5000 customers are mistakenly sent to the wrong mailing list with 1000+ recipients	Yes	Yes, report to individuals depending on the scope and type of personal data involved and the severity of possible consequences.	
A direct marketing email is sent to recipients in 'to' or 'cc' field, thereby enabling each recipient to see the email address of other recipients.	Yes, notifying the ICO may be obligatory if a large number of individuals are affected, if sensitive data are revealed (e.g. mailing list of a psychotherapist) or if other factors present high risks	Yes, report to individuals depending on the scope and type of personal data involved and the severity of possible consequences.	Notification may not be necessary if no sensitive data is revealed and if only a minor number of email addresses are revealed.

An individual phones to report having received a benefit letter intended for someone else. It is established that a personal data breach has occurred, and it is a systemic flaw so that other individuals are or might be affected.	Yes	Only the individuals affected are notified if there is a high risk and it is clear that others were not affected.	If, after further investigation, it is identified that more individuals are affected, an update to the ICO must be made and the additional step taken of notifying other individuals if there is a high risk to them.

Assessing the likelihood and severity of the risk to the rights and freedoms of data subjects

The type of breach	The type of breach that has occurred may affect the level of risk presented to individuals. For example, a confidentiality breach whereby medical information has been disclosed to unauthorised parties may have a different set of consequences for an individual to a breach where an individual's medical details have been lost and are no longer available.
The nature, sensitivity, and volume of personal data	Usually, the more sensitive the data, the higher the risk of harm will be to the people affected, but consideration should also be given to other personal data that may already be available about the data subject. For example, the disclosure of the name and address of an individual in ordinary circumstances is unlikely to cause substantial damage. However, if the name and address of an adoptive parent is disclosed to a birth parent, the consequences could be very severe for both the adoptive parent and child. Breaches involving health data, identity documents, or financial data such as credit card details, can all cause harm on their own, but if used together they could be used for identity theft. A combination of personal data is typically more sensitive than a single piece of personal data. Some types of personal data may seem at first relatively innocuous, however, what that data may reveal about the affected individual should be carefully considered. A small amount of highly sensitive personal data can have a high impact on an individual, and a large range of details can reveal a greater range of information about that individual. Also, a breach affecting large volumes of personal data about many data subjects can have an effect on a corresponding large number of individuals.
Ease of identification of individuals	An important factor to consider is how easy it will be for a party who has access to compromised personal data to identify specific individuals or match the data with other information to identify individuals. Depending on the circumstances, identification could be possible directly from the personal data breached with no special research needed to discover

	the individual's identity, or it may be extremely difficult to match personal data to a particular individual, but it could still be possible. Personal data protected by an appropriate level of encryption will be unintelligible to unauthorised persons without the decryption key. Additionally, appropriately implemented pseudonymisation can also reduce the likelihood of individuals being identified. However, pseudonymisation alone cannot be regarded as making the data unintelligible.
Severity of consequences for individuals	Depending on the nature of the personal data involved in a breach, for example, special category data, the potential damage to individuals that could result can be especially severe, in particular where the breach could result in identity theft or fraud, physical harm, psychological distress, humiliation or damage to reputation. If the breach concerns personal data about vulnerable individuals, they could be placed at greater risk of harm.
Special characteristics of the individual	A breach may affect personal data concerning children or other vulnerable individuals, who may be placed at greater risk of danger as a result. There may be other factors about the individual that may affect the level of impact of the breach on them.
Special characteristics of the data controller	The nature and role of the controller and its activities may affect the level of risk to individuals as a result of a breach. For example, a medical organisation will process special categories of personal data, meaning that there is a greater threat to individuals if their personal data is breached, compared with a mailing list of a newspaper.
The number of affected individuals	A breach may affect only one or a few individuals or several thousand, if not many more. Generally, the higher the number of individuals affected, the greater the impact of a breach can have. However, a breach can have a severe impact on even one individual, depending on the nature of the personal data and the context in which it has been compromised. The key is to consider the likelihood and severity of the impact on those affected.

Factors for considering a notification to data subjects:

Factor	**Impact on obligation to notify data subject**
Whether KCC has implemented and applied (to the affected personal data) appropriate technical and organisational protection measures—in particular measures that render the personal data unintelligible to any person who is not authorised to access it, e.g. encryption.	Where such measures have been implemented, it is not necessary to notify the data subject(s).
Whether KCC has taken measures following the personal data breach which ensure the high risk to the rights and freedoms of data subjects affected by that breach is no longer	Where such measures have been implemented, it is not necessary to notify the data subject(s).

likely to materialise.	
Whether it would involve disproportionate effort to notify the data subject(s).	If so, it is not necessary to notify the data subject(s)—but KCC must, instead, issue a public communication or similar measure whereby the data subjects are informed in an equally effective manner.
Whether there are any legal or contractual requirements to notify the data subject.	If yes, it may be necessary to notify the data subject(s) in any event.

Factors for considering a report to the ICO:

Factor	**Explanation**	**Typical Example(s)/ Report to ICO?**
The potential harm to the rights and freedoms of data subjects	This is the overriding consideration in deciding whether a breach of data security should be reported to the ICO. Detriments include emotional distress as well as both physical and financial damage. *The personal data breach **must be reported** unless it is unlikely to result in a risk to data subjects' rights and freedoms.*	-Exposure to identity theft through the release of non-public identifiers, e.g. passport number. **YES** -Information about the private aspects of a person's life becoming known to others, e.g. financial circumstances **YES**
The volume of personal data	There should be a presumption to report to the ICO where: —a large volume of personal data is concerned, and — there is a real risk of individuals suffering some harm It will, however, be appropriate to report much lower volumes in some circumstances where the risk is particularly high, e.g. because of the circumstances of the loss or the extent of information about each individual.	—loss of an unencrypted laptop holding names, addresses, dates of birth and National Insurance numbers of 100 individuals **YES** —loss of a marketing list of 100 names and addresses (or other contact details) where there is no particular sensitivity of the service being marketed **NO**

The sensitivity of data	There should be a presumption to report to the ICO where smaller amounts of personal data are involved, the release of which could cause a significant risk of individuals suffering substantial detriment, including substantial distress. This is most likely to be the case where the breach involves special category personal data. If the information is particularly sensitive, even a single record could trigger a report.	-theft of a manual paper-based filing system (or unencrypted digital media) holding the personal data and financial records of 50 named individuals **YES**

IG Library

Data Ethics

This guidance has been prepared in line with the Data Ethics Framework published by Central Government.

You can view the framework on this link Data Ethics Framework (publishing.service.gov.uk) and may benefit from completing it and scoring your project against the principles.

'Ethics' as a term refers to a set of moral principles or a system of moral values; it is a way of analysing what is deemed to be right or wrong behaviour and what our obligations are, both as human beings and as officers in a position of responsibility.

Ask yourself: just because we can, should we?

At KCC we have defined a set of Values and cultural attributes that set out who we are as people, what we stand for and how we will behave. These values are embedded into our culture and define how we work, setting a high standard for inclusion, diversity, taking personal responsibility, working better together and acting with compassion. When we work with data, personal or otherwise, how we behave should be no different.

When starting any project or new piece of work, you should be adopting an approach of 'data protection by design' and building processes and measures into your planning to ensure that KCC is working lawfully with the personal information entrusted to us. A large part of this is adopting an ethical approach to the use of data so that as a council we are confident that the work we do is transparent, accountable and fair.

The Principles of Data Ethics

The principles of data ethics much align with the first principle of the UK GDPR, to be 'lawful, fair and transparent'.

Transparency – this means that your actions, processes and data are made open to inspection by publishing information about a project in a complete, open, understandable, easily-accessible, and free format.

Accountability - this means that there are effective governance and oversight mechanisms for any project. Public accountability means that the public or its representatives are able to exercise effective oversight and control over the decisions and actions taken by the government and its officials, in order to guarantee that government initiatives meet their stated objectives and respond to the needs of the communities they are designed to benefit.

Fairness – this means that it is crucial to eliminate your project's potential to have unintended discriminatory effects on individuals and social groups. You should aim to mitigate biases which may influence your outcome and ensure that the project and its outcomes respect the dignity of individuals, are just, non-discriminatory, and consistent with the public interest, including human rights and democratic values.

The principles in practice

You should always have a clear understanding of what your project's purpose is and how it will benefit and affect the public.

As part of your planning, you must consider the following:

Who will be affected? And what are the needs of those people?

You must make sure that you understand the scope of your project and who could be affected by it, whether that is one person or a thousand people. You must also consider what the needs of those people are by asking the following questions –

- Is this work needed, and do we need to be interacting with this data for this purpose?
- What do any 'users' need from the project?
- Would there be any harm from not using this data?
- Have you considered Human Rights implications?
- Are there any environmental implications?
- What evidence do you have of the above?

Project plans should consider whether there could be any unintended or negative consequences of the work that is being proposed, and if so whether mitigations can be put in place to eradicate or minimise those consequences.

What are the benefits to both KCC and the wider public?

We must always be able to demonstrate the benefits of a piece of work, both to KCC and to the wider public. When approaching your work with data, make sure you consider –

- How you can measure and communicate the benefits to the public and make the work you are doing transparent
- What specific groups could benefit from the work.

Involve Diverse Expertise

Ensure that you have diversity within your project team as this helps to prevent biases and encourages more creativity and diversity of thought. You must also ensure that you have involved the right subject matter experts and practitioners.

- Have you involved external stakeholders and engaged in consultation? If so, what was the outcome and how has it shaped your work?
- Have you considered consulting with the target audience/users of the work you are proposing? This is invaluable in supporting you to ascertain the need and requirements of your project before you progress too far.

Do you have necessary and effective governance in place?

You must ensure that you are complying with relevant legislation and completing any necessary governance.

If you are using any personal data, you must ensure that you comply with the UK GDPR and the Data Protection Act 2018. This includes consulting with the Data Protection Officer and exploring the need for a Data Protection Impact Assessment.

You may also need to consider taking legal advice; at KCC you can contact the DPO to seek advice and request this.

In addition, you must consider the project's compliance with the Equality Act 2010. Using the information available on KNet, you should ensure that your work does not discriminate against any of the protected characteristics –

Age	Pregnancy and maternity
Marriage and civil partnership	Sexual orientation

You can do this by completing an Equality Impact Assessment (EqIA), which will help you to analyse your project and explore the risks and mitigations that can be put in place – check KNet for further information, guidance and a link to the app where you can carry out your EqIA.

Quality and Limitations of Data

You must ensure that the work you are designing has incorporated effective processes to ensure good data quality and integrity. This includes ensuring that you are complying with the data minimisation principle of the UK GDPR and only utilising the minimum amount of data possible to achieve your aims.

You should explore available options for minimising risks to the data you are working with, such as anonymisation and pseudonymisation. The bottom line is, can you still achieve what you need to with less identifiable data?

You should also ensure that you have built in an evaluation process as part of your project planning as this is crucial for establishing whether the measures that were put in place for the project were sufficient or whether further mitigations will be necessary for future projects. It will also help you identify ongoing considerations that may need to be taken.

Following evaluation, you should then look to document and share your learning to ensure compliance with the transparency principle. Methods of sharing would vary depending on the type of project but may include public engagement, a paper to a KCC Committee, a post on KNet etc.

Artificial Intelligence and Large Language Models (LLMs)

If you are considering the use of any form of AI tool or LLM etc, you must ensure that all relevant KCC policies have been followed, and that necessary governance is in place before proceeding with processing any data through the tool. This includes assessing all activity for the project, not just what information you plan to input; so, you must think about everything, such as how you sign up to use the tool in the first place.

Please ensure that you have read and understood KCC's AI Policy

Completing an EqIA and DPIA will assist you in exploring the ethics, proportionality and potential risks to the data. This may include –

- Bias – LLMs may return information from the internet that reflect historical practices that you would not want to replicate now, or the data may be a biased misrepresentation. What measures have you taken, or could you take, to mitigate bias?
- Discrimination – you must ensure that outputs do not cause indirect discrimination by the use of proxy variables for protected characteristics
- Individual rights – does the use of data in tools such as this interfere with the rights of individuals? If the answer is yes, is there a less intrusive way of achieving the objective?

IG Library

Legal Advice

There may be times when specialist advice is needed for a piece of work and consultation with legal professionals will be beneficial or required. This includes but is not limited to:

- Data Sharing Agreements
- International Data Transfer Agreements
- Data Processing Agreements
- Contracts
- Establishing roles and responsibilities in Controller and Processor relationships

Legal advice may be sought or recommended at any time, for example as part of the DPIA process or during procurement and can be obtained by first speaking with DPO Support who will be able to connect you with a colleague who can help.

It is important to keep in mind that legal advice often needs to be commissioned with an external firm, so it is vital that time constraints and budget are considered and planned for.

IG Library

Data Protection Impact Assessments (DPIAs)

DPIAs are a tool that can help assess the impact of data processing activities on the protection of personal data and identify the most effective way of complying with data protection obligations. An effective DPIA will allow KCC to identify and fix problems at an early stage, reducing the associated costs and damage to reputation that might otherwise occur. DPIAs are an integral part of 'data protection by design', another general legal obligation under UK GDPR, which is an approach that ensures privacy and data protection issues are considered at the early design stages of any system, product, service, or business practice, and then throughout its lifecycle.

Since 25 May 2018 conducting DPIAs has been mandatory in certain circumstances and this guidance will help you to determine when a DPIA must or should be carried out. It will be a key part of KCC's evidence that it is complying with obligations under the UK GDPR and the Data Protection Act 2018, including demonstrating that

privacy is an important consideration when data processing operations are being designed.

Non-compliance with DPIA requirements can lead to significant fines being imposed by the Information Commissioner's Office (ICO). The ICO has produced detailed Guidance for conducting a DPIA, which replaces the previous Code of Practice on conducting privacy impact assessments. Please see the ICO's DPIA Guidance

What is a DPIA?

A DPIA will help you to look at the objective of any project where you plan to process personal data. You will assess what the benefits to KCC and to data subjects are, identify any data protection risks and whether they can be mitigated and minimised, identify compliance risks and ultimately assess whether the level of risk is justified in the circumstances.

A DPIA must:

- describe the nature, scope, context and purposes of the processing
- assess necessity, proportionality and compliance measures
- identify and assess risks to individuals; and
- identify any additional measures to mitigate those risks.

In Short: DPIAs are a legal requirement and must be carried out where the data processing is likely to result in a high risk to the rights and freedoms of individuals. This is an essential part of demonstrating compliance with KCC's accountability obligations under UK GDPR.

When you need to carry out a DPIA

You must carry out a DPIA before you begin any type of data processing for which KCC is the data controller and which is 'likely to result in a high risk to the rights and freedoms of individuals'.

The term 'risk' in this context is about risk to individuals' interests and risks to their rights and freedoms, which includes risks to privacy and data protection rights and effects on other fundamental rights and interests (e.g. freedom of speech, prohibition of discrimination, etc.). A DPIA should therefore look at the risks from the data subject's perspective.

When assessing risk, and whether it is high risk, you will need to look at the likelihood and the severity of any potential harm to individuals. Something might be considered high risk because the potential harm is more likely, or the potential harm is more severe, or both. You also need to consider whether the proposed processing has any specific features which indicate a potential for high risk. If so, a DPIA will need to be carried out which will then analyse the risks, the likelihood and severity of any potential harm.

When you must carry out a DPIA

UK GDPR sets out three types of processing that automatically require you to carry out a DPIA. These are where you plan to:

- carry out any systematic and extensive profiling, on which decisions are based, which has legal effects or significantly affect individuals.
- process special category data or personal data relating to criminal convictions or offences on a large scale.
- systematically monitor publicly accessible areas on a large scale, (e.g., CCTV)

When using the KCC app to write a CCTV related DPIA, the app will generate specific questions to avoid users needing to complete a separate template. This should be completed in conjunction with the separate CCTV Policy and the Surveillance Commissioner's Code of Practice.

Other criteria which may indicate a likely high risk

Guidelines have also been published by the Article 29 Working Party ("the European Guidelines") with criteria which may indicate likely high risk. The ICO considers these guidelines to still be relevant since the end of the Brexit transition period as there have not been any significant changes to the UK data protection regime and they currently remain part of their guidance. These are:

- Evaluation or scoring: profiling and predicting behaviours. For example, screening customers against a credit reference database.
- Automated decision-making with legal or similar significant effect: for example, profiling which may lead to the exclusion of, or discrimination against, individuals.
- Systematic monitoring: for example, an employee monitoring program. The risk is increased where:
    - The individual may not be aware who is collecting their data or how it will be used; or
    - It is difficult for the individual to avoid being subject to such processing if the monitoring is in a public space.
- Sensitive data or data of a highly personal nature: the processing of sensitive personal data including special categories of data or data which more generally increases risks for individuals or impacts exercise of a fundamental right, such as location data or financial data. You should also consider personal data relating to criminal allegations, proceedings or convictions to fall within this criterion.
- Data processed on a large scale: the number of individuals concerned, the volume or range of different data items, the duration of the processing and its geographical extent are all potential components of this risk factor.

- Matching or combining datasets: where the datasets originate from different processing operations and data subjects could not reasonably expect them to be combined.
- Data concerning vulnerable data subjects: in cases where there is an imbalance in the relationship between the data controller and the data subject, meaning they may not be able to easily consent to or oppose the processing of their personal data. Vulnerable individuals may include children, individuals with mental or physical impairments, patients or the elderly.

> Note that employees also fall within the definition of vulnerable data subject in this context because of the imbalance of power in the relationship between employer and employee.

- Innovative use of technological or organisational solutions: the use of new technologies with novel forms of data collection and use or processing operations of a new kind where no DPIA has been carried out before by KCC.
- The processing prevents an individual from exercising a right or using a service or contract: including processing aimed at allowing, modifying or refusing individuals access to a service or entry into a contract. For example, a bank screens customers against a credit reference database to decide whether to offer a loan.

If at least two of the above criteria are met, this will indicate that a DPIA is required. However, the list above is not exhaustive; if there are other processing operations that may pose similar high risks, for example, the international transfer of personal data, particularly transfers outside of the EU, a DPIA should be conducted.

What the ICO considers likely to result in high risk

The ICO has published a list of processing operations which also require a DPIA, complementing the criteria set out in the European Guidelines. Some of the specified operations automatically require a DPIA, and some only when in combination with one of the other items, or any of the European Guideline's criteria:

Innovative technologies (use of innovative technology or the novel application of existing technologies (including AI))	A DPIA is required when combined with any of the criteria from the European Guidelines. It is KCC policy that all officers proposing to use personal data, and/or commercially sensitive data in an AI project or activity must complete a DPIA and EqIA and follow relevant processes with regard to ICT Compliance and Risk
Denial of a service (decisions about access to a	A DPIA is required.

service, product or opportunity based on automated decision-making (including profiling) or involves special category data)	
Profile individuals on a large scale	A DPIA is required.
Process biometric data	A DPIA is required when combined with any of the criteria from the European Guidelines.
Process genetic data (other than by an individual GP or health professional for provision of health care to the data subject)	A DPIA is required when combined with any of the criteria from the European Guidelines.
Data matching (combining, comparing or matching personal data obtained from multiple sources)	A DPIA is required.
Invisible processing (obtaining personal data from a source other than the individual without providing them with a privacy notice, if it is considered that to do so would prove impossible or involve disproportionate effort)	A DPIA is required when combined with any of the criteria from the European Guidelines.
Track individuals' location or behaviour (including but not limited to the online environment, data aggregation platforms, web and cross-device tracking, health or workplace monitoring, loyalty schemes)	A DPIA is required when combined with any of the criteria from the European Guidelines.
Targeting of children or other vulnerable individuals (use of personal data of children or vulnerable individuals for marketing, profiling or automated decision-making, or to offer online services or social networks to children)	A DPIA is required
Risk of physical harm (where a personal data breach could jeopardise an individual's physical health or safety)	A DPIA is required.

The ICO has produced within its DPIA Guidance a list of processing operations for which the ICO requires you to carry out a DPIA as they are likely to result in high risk. You should refer to this list of non-exhaustive examples to help better understand when a DPIA is required.

When a DPIA may not be required

A DPIA may not be required where:

- The processing is **not** likely to result in a high risk.
- The processing is on the basis of a legal obligation or public task, but only if:
    - there is a clear statutory basis for the processing.
    - the legal provision or a statutory code specifically provides for and regulates the processing operation in question.

    - there are no other obligations to complete a DPIA derived from specific legislation, such as Digital Economy Act 2017; and
    - a data protection risk assessment was carried out as part of the impact assessment when the legislation was adopted (the ICO recommends a DPIA is carried out in the absence of any clear and authoritative statement on whether such an assessment was done).
- The nature, scope, context and purpose of the processing are very similar to processing for which a DPIA has already been carried out.
- The processing is included on a list produced by the ICO of processing operations for which no DPIA is required - The ICO has not yet produced such a list but may do so in future.

If you establish that you are not obliged to carry out a DPIA, you must still continuously assess the risks around your processing activities to identify when a type of processing is likely to result in a high risk to the rights and freedoms of individuals and keep it under review. Where it is determined that a DPIA does not need to be carried out, a record should be kept of the reasons why a DPIA was not considered necessary.

The Data Protection Officer's advice should be sought on whether you need to do a DPIA. This is done via the screening tool on the KCC App, which helps you determine whether the proposed processing is of a type that is likely to result in a high risk and, therefore, if you are required to carry out a DPIA. Even if no mandatory obligation to carry out a DPIA applies, you must still properly consider whether the proposed processing is likely to result in a high risk and, if it is considered it has features which indicate a likely high risk, you should carry out a DPIA.

If you are not sure whether the processing is likely to result in a high risk, you should carry out a DPIA regardless.

DPIAs and Data processing prior to GDPR

Where your data processing already existed prior to GDPR coming into force, you should review those processing operations to identify whether they would be considered likely to result in a high risk under UK GDPR. You can use the DPIA screening tool to do this.

If the risks have not already been adequately assessed, then you may need to carry out a DPIA to ensure the processing is compliant with UK GDPR. If you have already considered the relevant risks and safeguards of your data processing, whether that was through a 'privacy risk assessment' or other type of risk assessment process, then you may not need to carry out a DPIA, unless the nature, scope, context or purposes of the processing have significantly changed since that previous assessment was completed. In case of any challenge, you should keep a

written record of the review carried out and any reasons for determining that a new DPIA is not being carried out.

Roles and responsibilities in the DPIA process

The data controller is responsible for a DPIA, so where KCC is a data controller, it will be responsible for considering whether a DPIA is required and ensuring that a DPIA is carried out.

A DPIA may be outsourced or carried out by a data processor if they will be doing the processing on behalf of KCC, but KCC ultimately remains responsible for it, and it must still be sent to the DPO for review and advice.

If a processing operation involves a joint data controller, the respective obligations of the data controllers will need to be precisely defined and the DPIA will need to clearly set out which data controller is responsible for the particular measures identified to address any risks identified. Each data controller should express their requirements/needs and share information without compromising secrets or confidential business information or disclosing vulnerabilities.

In most cases, it is likely that it will be most appropriate for project or operational managers to carry out the DPIA, with senior managers having oversight of the project.

Information Asset Owners are responsible for signing off DPIAs. Where a DPIA concerns the use of staff personal data (for example, in any proposed restructure where salaries will be processed), then both the IAO for the relevant service area and the IAO responsible for HR matters should sign off the DPIA.

There are, however, others who you should involve and consult with, depending on the nature of the project, which might include:

- Data Processors – where the processing is partly or wholly performed by a data processor, the processor should assist KCC and provide any necessary information to KCC in carrying out the DPIA.
- Information security teams (for example, ICT Compliance and Risk if there are technical aspects to the project).
- Legal advisers.
- Other experts, such as IT experts or any other professional.
- Data subjects or their representatives – you must seek the views of data subjects or their representatives where appropriate. This could be done through various means (e.g. a study or survey, questions to staff), ensuring that you have a lawful basis for processing the personal data when seeking the views of data subjects. If you do not seek the views of data subjects, you must record the reason why in the DPIA, for example, seeking the views of data subjects would compromise confidentiality of business plans, undermine security, or would be disproportionate or impracticable. If your views/decision

are different from the data subjects' views, then you must record the reasons for going against their views in the DPIA.

- Other internal business units or external stakeholders involved with the project.
- Senior Information Risk Owner (SIRO) – for example, you must consult with the SIRO where any residual high risks have been identified.
- The Caldicott Guardian - where confidential patient information (which includes social care clients) is being used or disclosed.
- The Data Protection Officer (in all cases - see below).

The role of the Data Protection Officer (DPO)

When carrying out a DPIA you must seek the advice of the DPO. The DPO will provide you with advice on:

- whether you need to do a DPIA
- how you should do a DPIA
- whether to outsource the DPIA or do it in-house
- measures and safeguards to mitigate risks
- whether the DPIA has been completed correctly
- the outcome of the DPIA and whether the processing can go ahead.

The advice given by the DPO must be documented in the actions section of the DPIA app, together with the decision of KCC (as signed off by the Information Asset Owner). If the decision is to go against the advice of the DPO then this must be justified and the reasons for doing so must also be clearly recorded.

You should contact the DPO as early as possible in the process for advice regarding a DPIA. It is not acceptable to seek advice from the DPO on a DPIA at the point you intend to start the processing as this goes against the principle and legal requirement of data protection by design.

When you must consult with the Information Commissioner's Office (ICO)

If you have carried out a DPIA which reveals a high risk to individuals which cannot be reduced or mitigated, or because the costs of mitigation are too high, the Information Commissioner's Office must be consulted before you can go ahead with the processing. You should also notify and consult the SIRO in advance that you have decided or been advised that the high risks cannot be mitigated and notification to the ICO is required. The DPO will refer the matter to the ICO.

Upon accepting a DPIA for consultation, the Information Commissioner's Office will then have 8 weeks to provide written advice, which can be extended by a further 6 weeks if the processing is complex. The DPIA cannot be approved before a response has been received from the ICO.

Examples of when there might be a high residual risk include:

- where the data subjects may encounter significant, or irreversible, consequences, which they may not overcome
- when it seems obvious the risk will occur.

The ICO may take the view that the processing can proceed, or they could provide advice on how the risks can be further mitigated before the processing starts. If the ICO is concerned that the proposed processing is likely to contravene UK GDPR, then they will issue an official warning, together with recommended steps on how to avoid any contravention of UK GDPR. If the ICO has more significant concerns, they may impose a limitation or ban on the proposed processing.

The DPIA process

The DPIA should be started as early as possible in the design stages of the proposed processing and must be carried out prior to the start of the processing. The DPIA should be carried out alongside the planning and development of the project and updated throughout the lifecycle of the project.

In some circumstances not all the necessary information may be available at the start of the project and certain decisions can only be made at a later date, or the project may be being undertaken in phases. The DPIA must therefore be kept under review and be regularly reassessed and should be considered a living document which may need regular updating.

A DPIA is a continual process from the start of any project planning and throughout the life of the project, and so it is not acceptable to postpone or not carry out a DPIA because it might need to be updated later.

DPIAs must also be considered if any changes are being made to an existing system. If any significant changes to the processing, or new/increased risks to individuals are identified then advice from the DPO should be sought.

A DPIA will normally relate to one project/processing operation. However, there may be scenarios where a single DPIA can be used to assess multiple processing operations that are similar in terms of nature, scope, context purpose and risks. For example, where similar technology is used to collect the same sort of data for the same purposes, for example, for ANPR cameras in various car parks. A group of data controllers may also carry out a joint DPIA for a group project or industry-wide initiative.

Where you are proposing to implement a new technology, it is worth asking the product developer if they have their own DPIA in relation to the technology/product, as this can inform KCC's DPIA.

A record of the DPIA should be retained for the lifetime of the system or project/processing and be regularly reviewed and updated, when necessary.

What a DPIA must include

As a minimum the DPIA should include:

- A description of the processing operations and the purposes. You should include enough detail for the data flow to be easily understood and scrutinised for any further possible mitigation measures which will improve data protection.
- An assessment of the necessity and proportionality of the processing in relation to the purpose.
- An assessment of the risks to individuals.
- The measures in place to address and mitigate any risk, including security and to demonstrate that you comply with UK GDPR (e.g. staff training, pseudonymisation or anonymisation of data according to KCC's anonymisation and pseudonymisation policy and any IT security measures in place. These should cover organisational and technical measures that are both generally in place within KCC and those that are specific to the project).

Your DPIA will be reviewed by the DPO support function to ensure it is completed as fully as possible before recommendations are issued. If you decide not to follow the advice of the DPO, you must justify this position and record your reasons in the DPIA.

Once the DPO has provided any advice, you should integrate the outcomes and action points in the DPIA into your project planning and ensure the actions are implemented.

If you identify that any high risks assessed cannot be mitigated, then you must consult the ICO before any data processing starts (see section above).

You will need to keep the DPIA under review throughout the life of the project and processing and monitor its performance. It is recommended that you agree and document a schedule for reviewing the DPIA regularly. In addition, if there is any significant change in the nature, scope, context, or purposes of the processing, then the DPIA must be reviewed and the steps in the DPIA process repeated.

Whilst any risks will be documented within the DPIA, project managers will also need to record any material privacy-related risks as part of the project or service/divisional risk register and have regular monitoring arrangements in place. If you require any advice in this regard, you can refer to the KCC Risk Management Toolkit on KNet.

IG Library

Individual rights

All data subjects, (including KCC staff) have the following rights in relation to their personal information:

- to be informed about how, why and on what basis that information is processed. This right is met by providing individuals with an effective Privacy Notice.
- confirmation that personal information is being processed and to obtain access to it and certain other information. Individuals can exercise this right by making a Subject Access Request.
- to have personal information corrected if it is inaccurate or incomplete. We should make every effort to accurately record data and ensure that correction is possible on systems we use.
- to have personal information erased if it is no longer necessary for the purpose for which it was originally collected/processed, or when the consent on which the processing is based has been withdrawn and there are no overriding legitimate grounds for the processing. This is often referred to as 'the right to be forgotten'.
- to restrict the processing of personal information and limit the way a Data Controller can process their data. Data subjects can exercise this right by asking us to stop using their data for specific reasons.
- in limited circumstances, to receive or ask for their personal information to be transferred to a third party in a structured, commonly used and machine-readable format. Data subjects can exercise this right by asking for their information to be seamlessly transferred to another party. This is not something that often applies to local authorities but can be relevant in situations such as changing your mobile phone provider or changing your gym.
- where processing of personal information is based on consent, to withdraw that consent at any time. This means that where KCC is relying on consent as it's lawful basis, it must be possible for that consent to be withdrawn and for the processing to stop.
- to request a copy of an agreement under which personal information is transferred internationally. Where we enter into agreements relating to transferring information out of the UK, we must be able to provide a copy to the data subject on request.
- to object to decisions based solely on automated processing, including profiling. This means, where automated decision making is taking place, such as by the use of computer algorithms, the data subject can ask that the decision be reviewed by a person.
- to be notified of a data breach which is likely to result in high risk to their rights and obligations. This means, if we become aware of a personal data

breach that may have a significant impact on a data subject, they have a right to be informed about it.

- to make a complaint to the ICO or a Court. Data subjects have the right to make a complaint to the Information Commissioner or a Court at any time if they are unhappy with the way their information has been processed.

KCC's Privacy Notice template includes details of these rights and advises data subjects wishing to exercise their rights to contact the Information Resilience & Transparency team via email: dataprotection@kent.gov.uk.

Important: Unless there is a statutory basis for KCC to do so, individuals may object to KCC's use of their information. Objections will be recorded and respected and the individual informed of any consequences, for instance it may mean KCC is unable to provide a specific service.

IG Library

Records Management

KCC is committed to creating, keeping and managing data, information and records which document its principal activities. This guidance covers data, information and records regardless of the media in which it is stored (i.e. physical or digital formats - including e-mails) which are deemed to be part of the corporate record. This includes all data, information and records created by KCC including those created by contractors and partners working on KCC's behalf regardless of where they are created, stored or managed.

Effective data, information and records management:

- is at the core of every service provided by Kent County Council (KCC) whether directly to the people of Kent or as an internal support service.
- supports the implementation of KCC's strategies and ensures that KCC creates data, information and records which are accurate, reliable and accessible.
- ensures that KCC can meet government requirements for open data and transparency.

This section contains overarching requirements to ensure that KCC:

- creates and manages accurate, authentic, reliable and accessible data, information and records to meet the authority's business needs.
- identifies data, information and records which should be disposed of and disposes of it in line with KCC's information security requirements.
- includes all business-critical data, information and records in business

- continuity plans.
- can identify information which could be published as part of the Open Data and Transparency programme.

This section also identifies the requirements to bring about these outcomes but does not include any information about how to fulfil the requirements. The Information Management Manual contains all the information members of staff will require to implement this guidance.

Roles and Responsibilities

All KCC employees are responsible for creating and maintaining data, information and records in relation to their work that are authentic and reliable.

It is the responsibility of each Service Unit to identify staff with specific responsibilities for information management in the Service Unit and these responsibilities should be defined in their job descriptions.

The head of each directorate is the Information Asset Owner for their directorate.

The Head of Libraries Registration and Archives is responsible for managing the day to day running of the Records Management Service. However, the Records Manager is responsible for ensuring that the Records Management Service remains compliant with current record keeping practices.

Record Creation and Storage

[See sections 7-8 of the Information Management Manual]

All KCC staff are responsible for creating and maintaining data, information and records in relation to their work and storing them in a way that ensures they can be identified and retrieved when required using the methods laid out in the Information Management Manual.

Individual directorates must provide for the preservation and secure storage of all data, information and records regardless of the format in which they are stored in until they can be safely disposed of. Records storage space in occupied office buildings must meet the specification laid down in the Information Management Manual. Principal copies of semi-current records should, where there is no available office space, be transferred to the Records Management Service until they have reached the end of their statutory retention period. The Records Manager is the trusted custodian who is responsible for the management of inactive data, information and records held in physical format where the information asset owner cannot be identified.

Information Communication Technology

This policy refers to the appropriate technical policies which establish the criteria applied to electronic systems which process and store records.

Digital Continuity

[See Specialist Guidance 3 in the Information Management Manual]

It is the responsibility of each Directorate to ensure that all digital data, information and records which must be kept for longer than 7 years meet the requirements of the Digital Continuity policy and that the relevant resources provided to do this.

The Records Manager is the trusted custodian who is responsible for the management of inactive data, information and records held in electronic format where the information asset owner cannot be identified.

Record Retention and Disposal

[See section 9 of the Information Management Manual]

All data, information and records (regardless of the media in which they are stored) must be retained for the period identified in the corporate retention schedule.

The retention periods listed in the schedule are the minimum length of time which the data, information and records must be kept. Where necessary data, information and records may be kept for longer periods of time.

It is the responsibility of each directorate to identify those members of staff who are responsible for identifying and disposing of obsolete data, information and records in an auditable manner. The disposal of all data, information and records must follow the requirements outlined in section 9.4 and 9.5 of the Information Management Manual.

Business Continuity

Individual service units are responsible for identifying the data, information and records (regardless of the media in which they are stored) which are considered to be business critical and to ensure that the business-critical elements are included in individual service unit business continuity plans. Individual service units are also responsible for specifying operating parameters (extent and frequency) of the backup copies taken of the data, information and records such that they are fit for purpose.

It is the responsibility of ICT to ensure that backups are created to the agreed standards and to establish an effective back-up restoration regime to ensure that when backups need to be restored, they remain fit for purpose.

IG Library

Information security

KCC applies a risk management approach to information security. This identifies information assets on which KCC is dependent and assesses risks to their

confidentiality, integrity and availability. Personal data is protected in accordance with the principle of 'integrity and confidentiality' as required by the UK GDPR.

KCC seeks to promote a culture that properly values, protects, and uses information for the public good.

Principles of information security

a) Information security is part of KCC's wider information governance management and policy framework, and the approach is based on published good practice.
b) KCC defends its information against common threats such as opportunistic hackers and abuses of business processes, while remaining proportionate and aligned with wider business goals.
c) KCC's risk-management approach to information security assesses risks to the confidentiality, integrity, availability, and resilience of information and to the processes and services involved in the processing of that information.
d) KCC considers the nature, scope, context and purposes of processing personal information as well as the likelihood and severity of any risks involved to the rights and freedoms of individuals.
e) KCC implements measures to ensure a level of security appropriate to the risk, including:
    - the pseudonymisation and encryption of personal data
    - capability to facilitate the availability and access to personal data in a timely manner in the event of a physical or technical incident
    - a process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing.
f) Information security controls are based on ISO27002 (Code of Practice for Information Security Controls) and consider:
    - the sensitivity and value of information
    - the impact or harm that may result should an incident or event occur.
g) Managers are responsible for ensuring that those handling personal and confidential information are competent to do so and are supported by robust policies and procedures.
h) Contractors are held to account under contract terms required by law for their handling of KCC's personal and confidential information.
i) Personal and confidential information are only to be shared with external partners in ways that are secure, fair, transparent, and lawful.
j) KCC responds promptly and effectively to information security incidents and has a Data Breach Policy to ensure all personal data breaches are notified appropriately and without undue delay. KCC will use appropriate technical and organisational measures in accordance with its Information Security Policy to

keep personal information secure, and, to protect against unauthorised or unlawful processing and against accidental loss, destruction or damage.

KCC will develop, implement and maintain safeguards appropriate to its size, scope and business, its available resources, the amount of personal information that it owns or maintains on behalf of others and identified risks (including the use of encryption and pseudonymisation where applicable). It will regularly evaluate and test the effectiveness of those safeguards to ensure security of processing.

All staff are responsible for protecting the personal information KCC holds. Staff must guard against unlawful or unauthorised processing of personal information and against the accidental loss of, or damage to, personal information. Staff must exercise particular care in protecting sensitive special category personal information from loss and unauthorised access, use or disclosure.

Staff must follow all procedures and technologies put in place to maintain the security of all personal information from the point of collection to the point of destruction. Staff may only transfer personal information to third-party service providers who agree to comply with the required policies and procedures and who agree to put adequate measures in place, as requested.

Staff must maintain data security by protecting the confidentiality, integrity, resilience and availability of the personal information, defined as follows:

a) Confidentiality - only people who have a business need and are authorised to use the personal information, can access it.
b) Integrity: personal information is accurate and suitable for the purpose.
c) Availability: authorised users can access the personal information when they need it for authorised purposes.

Staff must comply with and not attempt to circumvent the administrative, physical and technical safeguards KCC has implemented and maintains in accordance with the UK GDPR.

Where KCC uses external organisations to process personal information on its behalf, additional security arrangements must be implemented in contracts with those organisations to safeguard the security of personal information. Contracts with external organisations must provide that:

- the organisation may only act on the written instructions of KCC,
- those processing personal information are subject to the duty of confidence,
- appropriate measures are taken to ensure the security of processing,
- sub-contractors are only engaged with the prior consent of KCC and under a written contract,

- the organisation will assist KCC in allowing individuals to exercise their rights in relation to data protection,
- the organisation will delete or return all personal information to KCC as requested at the end of the contract,
- the organisation will submit to audits and inspections, provide KCC with whatever information it needs to ensure that both parties are meeting their data protection obligations, and tell KCC immediately if it is asked to do something infringing data protection law.

These terms are set out in Article 28 of the UK GDPR, and you may hear reference to an 'Article 28 compliant contract'. Before any new agreement involving the processing of personal information by an external organisation is entered into, or an existing agreement is altered, the relevant staff must seek approval of its terms from a relevant contact in Commissioning.

Information risk management

Information risk is managed by the SIRO (Senior Information Risk Owner) who has corporate oversight of information risks associated with KCC's information assets. Corporate Directors are responsible for managing risks associated with assets within their service areas.

Information assets

For management purposes each key business information system is an 'information asset'. Each asset is accredited as meeting KCC's information security requirements, either at service commencement or through a documented information risk assessment.

The Records Manager is responsible for maintaining the Corporate Information Asset Register (CIAR) for the SIRO and the Register of Processing Activities (ROPA) for the DPO. The Chief Information Security Officer is responsible for ensuring each asset is accurately documented with:

- technical overview and description
- details of contracted third parties who manage or provide the asset
- ICT risk assessment
- risk-review statements.
- the assigned Information Asset Owner (IAO).

ICT information risk assessment

- ICT Information risk assessments must be completed by a 'competent person' and can be sought via ICT.
- Residual information risk(s) that exceed corporate risk tolerances after recommended controls are implemented must be considered by the relevant IAO.

- ICT Information Risk Assessments are held by the ICT Compliance and Risk Manager
- Risk Assessments and summary risk statements are sent to Information Asset Owners.

Secure data handling

Most routine handling of personal and sensitive information uses digital applications and services provided by KCC's ICT service provider(s) which are designed with appropriate security. Information sent or moved beyond KCC's network is likely to leave its security control. There are legal restrictions on when and how personal information can be shared.

If in doubt, seek advice from the DPO or from the Information Resilience and Transparency Team.

Principles:

(a) If sending personal or sensitive information, check the recipient's address. If using email, identify a suitable method from the Secure Email Policy and the Specialist Guidance in the Information Management Manual on Managing Email. If using another method, ensure it is secure and if in doubt, seek advice.

(b) If communications are generated by an automated IT system, or mail-merge is used, check before sending to ensure the right recipient receives the right information.

(c) Those sending personal or sensitive information must have completed mandatory data protection and information governance training.

(d) Those sending personal or sensitive information must be confident that the recipient will handle the information in a secure and proper manner.

(e) Managed printers have 'follow-me' features, which means documents are only printed in the presence of the authorised user, reducing the risk of being left unattended or sent to the wrong printer. Bear in mind that should a printer jam or run out of ink for instance while printing your document, you should not abandon it, as when the issue is resolved the printout will be produced.

(f) Those handling personal or sensitive information must be mindful of the safeguards and controls set out in KCC's Information Management Manual, in particular the sections covering Information Security, Retention and Disposal.

(g) Those handling personal or sensitive information should use measures such as pseudonymisation and encryption where appropriate.

Those receiving personal or sensitive information from external sources (for example CJSM or Public Health) must handle the information in accordance with the terms and conditions of its use.

ICT security

KCC's ICT systems and services are certified by the Public Service Network Agency as appropriate. This requires policies designed to control specific risks relating to ICT security; these can be found on KNET under relevant headings. The following highlights those applicable to most users.

a) Access to KCC's ICT systems must be authorised by an appropriate manager. If an employee, this will be their line manager. If a contractor, this may be the relevant contract manager.
b) All employees are required to comply with the ICT Acceptable Use Policy as a condition of service. Access to personal information held by KCC is only permitted for professional reasons. Negligent and/or deliberate misuse of ICT equipment or resources will result in disciplinary action and in some cases dismissal or criminal prosecution (such as inappropriate or unauthorised use of information leading to offences under the Computer Misuse Act 1990 or the unlawful obtaining, disclosing or retaining of personal data without the consent of the data controller under the Data Protection Act 2018).
c) Users are responsible for keeping their password secure and must not disclose or share it. Employees are accountable for activity on their user account.
d) Most data breaches are caused through human error and training and awareness raising are the best line of defence to reduce this. Think before you click.
e) Screens must be locked when employees are away from their computers.
f) KCC's mobile devices must be cared for and not left unattended in public places or visible in a parked car.
g) If using a personal device, staff must not circumvent controls that are in place to protect KCC's information and must abide by KCC's BYOD Policy. Staff must report any loss or theft promptly.
h) Staff must follow KNet guidance, the ICT Acceptable Use Policy and the specialist guidance in the Information Management Manual on removing physical records from KCC premises and working remotely.
i) When storing data electronically outside of KCC's server environment, staff must abide by the council's ICT Acceptable Use Policy
j) Where cloud services are being used, it is essential the personal data is stored within the UK or other recognised domain using the ICO model clauses or which has been determined by the Secretary of State to have adequate data protection law and follows cloud security principles. Staff should refer to the ICT Acceptable Use Policy for further information.

Physical and environmental security

The physical and environmental security of KCC's buildings and premises is managed by facilities contractors. Managers are responsible for the training and security policies and the practices of their employees.

a) ID cards must be worn, and visitors issued with a temporary pass and escorted during their visit. Those not wearing badges or seen ‘tailgating’ should be challenged.
b) Desks must be clear of personal and sensitive information when unattended. Documents containing personal or sensitive information must be locked away when not in use.
c) Managers should undertake periodic confidentiality surveys, the results of which should be used to inform improvements.
d) Areas where Confidential Information is processed or handled should be treated as Safe Havens.
e) The risks to paper records should be assessed periodically and when significant changes to the physical environment are proposed as they may be vulnerable to environmental risks such as water or fire or may be left in abandoned buildings.
f) The physical and environmental security of ICT equipment (not user devices) is assessed at installation and reviewed annually.

Mobile and hybrid working

KCC now operates a hybrid working arrangement which means that many colleagues are regularly working from home. The principles of Data Protection remain the same wherever you are based, and staff must ensure that all available mitigations are taken to keep information safe and secure. This can mean measures such as:

- Keeping laptops, paperwork and diaries etc locked or packed away out of sight when not in use and protecting them in transit, e.g. concealed in a car boot
- Keeping hard copy paperwork to a minimum
- Being mindful of where you are and who may overhear what you are saying.
- Taking care to avoid other household members seeing what you are working on
- Using a headset to minimise the risk of other parties being overheard.

Employees who access their work away from the office must do so within the terms and conditions of the Using IT Equipment for Remote Mobile Working Policy and Standard and ‘5 steps to Managing Homeworking and Physical Records Safely’. These guides are available on KNet.

Employment starters and leavers

a) Appropriate background checks are carried out during recruitment (including temporary workers) and prior to appointment, with vetting for sensitive and regulated roles.
b) A checklist and guidance for managers and those employing contractors ensures all new starters complete mandatory training, including information governance and data protection modules.

c) All new employees sign to confirm they understand their employment Terms and Conditions (Blue Book) and the Kent Code (Code of Conduct). Both documents include sections on information security. The Code confirms that inappropriate disclosure of information will render staff liable to disciplinary action and could lead to criminal prosecution.
d) Managers must authorise access to ICT systems and services, and for sensitive applications, additional training is mandatory before access is approved.
e) Managers requesting user accounts for temporary workers must provide an end date. Access to ICT services may be automatically revoked when temporary workers reach this end date unless expressly renewed by the line manager requesting an extension.
f) Whether accidental or deliberate, employees and contractors can pose a potential threat to the security of KCC's information. The line manager is best placed to pick up and act on indications that may cause concern and respond appropriately.
g) A checklist and guidance for managers ensures that user accounts are rendered inaccessible when an employee or temporary worker leaves employment. Managers must ensure that when staff leave or move to new roles the access rights of those staff are updated.

Business Continuity

Business Continuity Plans should be in place for all critical information assets, with relevant employees aware of their roles and responsibilities.

Contract managers are responsible for monitoring contract performance, including data protection compliance and must be able to provide evidence of this. They should refer to ICO guidance for further information. Where a contractor is unable to demonstrate that their information security measures are adequate, restrictions must be considered, such as the use of secure email, until improvements are made. A failure to ensure a contractor has adequate security measures in place as required by the UK GDPR exposes KCC to the risk of a significant fine.

Information security incidents

KCC has an incident reporting system that must be used promptly when reporting information security incidents as set out in the Data Breach section.

Monitoring

Information security is monitored and reported through the following:

a) Information Governance Cross-Directorate Group
b) Internal audit - There is an annual cycle of audits that cover areas of the business deemed to represent the greatest risk to the council. This includes information security, and risks are reported to the Governance and Audit Committee.

c) Data Breach Register - This is owned and monitored by the DPO as part of the role's compliance duty.

IG Library

Information Sharing

'Information Sharing' is the disclosure, exchange or pooling of personal information between organisations and agencies. There are a wide range of reasons why information is shared and often it is for more than one purpose. Those purposes must by law be set out in a privacy notice provided to the individual at the time the data is collected. People generally expect organisations to share their personal information to provide joined-up services; it is part of the way KCC works and should be approached with confidence.

CTRL Click Information Sharing if you would prefer to watch a short video that takes you through the basics of Information Sharing

Broadly speaking an individual's personal safety is more important than protecting their personal data. In an emergency e.g. where there is a risk of serious harm to human life, data should be shared as is necessary and proportionate. Such scenarios should be anticipated as part of business planning. Document the action taken after the event if it can't be done at the time.

Scope

This guidance applies to personal data shared with partners, statutory agencies or internal divisions including:

a) routine or systemic sharing for an established purpose
b) an exchange of information between organisations
c) one-way, exceptional or ad hoc sharing in response to requests or in an emergency
d) several organisations pooling information and making it available to each other or a third party
e) providing access to a third party via IT systems.

This guidance does not apply to personal data that is:

a) processed by contracted third parties acting on KCC's behalf (data processors), as these are bound by terms and conditions of their contract with KCC and must only process personal data on documented instructions from KCC.
b) effectively anonymised.

This guidance assumes that parties who share information do so as data controllers.

The means of transfer may be physical or digital, including (but not limited to) email, fax, post, online portal, information system or electronic file transfer.

Fair and Transparent

Sharing must be fair and transparent which means individuals must understand how their personal information is used. Ensure that you are adhering to the guidance in the sections above about the principles of data protection and how we provide Privacy Notices.

Lawful

Information sharing must be lawful:

a. A lawful basis on which information is shared must be identified in the UK GDPR and be documented before personal data is disclosed or released.
b. Special categories of personal data should not be disclosed without one of the limited lawful grounds identified in the UK GDPR.
c. In addition to identifying a lawful basis under data protection law, data sharing must also be lawful in a general sense. This means checking that KCC has the legal power to share data. KCC derives its powers and duties from Acts of Parliament, or regulations, or from case law, or under common law. These can define the function and purposes for KCC's data sharing and could be:
    i. express statutory obligations to share (usually highly specific circumstances)
    ii. express statutory powers to share such as the 'gateways' to share in defined purposes such as detecting fraud under the Digital Economy Act 2017
    iii. implied statutory powers where it may be possible to rely on an implied power to share, which is derived from express provisions of legislation by authorising activities which are reasonably incidental to those which are expressly permitted. KCC often relies on the 'public task' lawful basis which requires a legal power to be laid down by law. This does not need to be in an explicit Act or regulation, but could be a common law task, function or power, so long as it is sufficiently foreseeable and transparent.
d. Whatever the source of the legal basis, KCC must check that the power covers the specific disclosure or data sharing arrangement. If it does not, information must not be shared, unless, in the circumstances, there is an overriding public interest in a disclosure taking place.
e. KCC must comply with the Human Rights Act 1998 when carrying out its functions. It must not act in a way that would be incompatible with rights under the European Convention on Human Rights. Article 8, which gives everyone the right to respect for their private and family life, home and correspondence, is relevant to sharing personal data.
f. A duty of confidence may be stated explicitly, or it might be implied (as it was collected in circumstances where confidentiality is expected e.g. medical or

banking information). You should consider obtaining legal advice on your data sharing plans.

g. Health and social care data are recognised in the Health and Social Care Act 2012 as 'Confidential Information' that may be shared for direct care, support and case handling unless the individual objects.
h. Objections must be respected unless there is a statutory justification.

Sharing for secondary purposes must be approved on a case-by-case basis by KCC's Caldicott Guardian. All purposes for individuals' data sharing should be identified at the point of collection within the relevant service's privacy notice.

When KCC is acting as a competent authority (e.g. Trading Standards) sharing data for law enforcement purposes (e.g. preventing or detecting crimes) will be subject to Part 3 of the DPA 18 and not the UK GDPR. There are some similarities with UK GDPR requirements but also differences such as the requirement for automated systems to clearly distinguish between different categories of data subjects i.e. suspects, convicted criminals, victims and witnesses. Detailed records of all data processing activities must be kept and any IT database for data processing must keep logs for specific processing operations such as collection, alteration, erasure and disclosures (including transfers).

Documented and accountable

Information sharing should be documented and accountable.

A data sharing agreement (DSA) sets out the purpose of the sharing, covers what will happen to the data at each stage, sets standards, helps all the parties to be clear about their roles and demonstrates accountability. It should be noted that a DSA is different to a Data Processing Agreement, which is an agreement that can be put in place when data is being given to a third-party processor to work with on our behalf.

a) All new information sharing arrangements must be screened for their potential impact on individual privacy.
b) The Data Sharing Code of Practice recommends carrying out a Data Protection Impact Assessment (DPIA) if a major project involves disclosing personal data, or an organisation plans routine data sharing.
c) Routine information sharing must be documented to an acceptable standard, and documentation made available for inspection and audit.

The agreement must be clear and set out:

- Who is sharing and what is their role? – Identify all organisations involved in the agreement and their role
- What is the purpose of the sharing? – Clearly state the aims and why the data sharing is necessary

- Which other organisations are involved? Are you a joint controller? If so, you must, by law, set out your responsibilities under both the UK GDPR and DPA 18 and indicate a contact point for individuals.
- What are you sharing? Set out the types of data shared in detail. Ensure only the specific data that is needed to achieve KCC's clear objectives is shared and is accurate.
- What is the lawful basis for sharing? Set out KCC's lawful basis for sharing. This may be different to the basis used by your partner. If consent is to be used as a lawful basis, provide a model consent form and address how consent is withdrawn. Set out KCC's legal power to share.
- Are you sharing special category or criminal offence data? Document the relevant Article 9 condition and any further conditions under the DPA 18.
- How will individuals access their data? Include how requests from individuals will be dealt with (whether under FOI or UK GDPR) but state that all controllers remain responsible for compliance.
- How will individuals be given information about the use of their information? Ensure the organisation or person receiving the data provides the individuals with a privacy notice, unless an exception under the UK GDPR applies.
- How will information be secured? Ensure the recipient can provide a suitable level of information security and has taken appropriate technical and organisational measures to protect the personal data.
- How will information governance be dealt with? Ensure there is a mutual obligation of co-operation in relation to UK GDPR compliance and expected standards and procedures are set. Refer to other sections of this policy for details and expected standards.

When an arrangement commences or ends the relevant service must notify the appropriate Information Governance Lead. All information sharing agreements must be recorded centrally within KCC's Record of Processing Activities (ROPA) by sending them to the Records Manager.

Services should have a mechanism in place to monitor the arrangements that are in place. All information sharing agreements must be reviewed on an annual basis to ensure that the data is still needed and its use justified.

KCC is a signatory to the Kent and Medway Information Sharing Agreement (KMISA) which provides for openness and transparency in information sharing, as well as appropriate governance and support, to assist signatory organisations to share personal information lawfully, safely and securely.

A signatory to the KMISA KCC is expected to share personal information with other signatories in accordance with the provisions of the agreement underpinned by a record of sharing (for repeat or single use) and there should be no need to enter into sub-agreements to share personal information.

Necessary and Proportionate

Information sharing must be necessary and proportionate and the impact on individual privacy and confidentiality understood.

a) The proportionality of the data sharing and the potential harm to individuals should be central to the analysis.
b) Consider whether it is necessary to share personal data at all. If possible, use anonymised information instead.
c) When deciding whether to enter into a data sharing arrangement, consider if it is:
    - right to share that data in a particular way
    - the action of a responsible organisation
    - reasonably expected by data subjects
    - properly justified.
    - likely to adversely affect individuals and
    - subject to clear and strong safeguards.
d) Ethical principles form part of considerations on proportionality and fairness and are complementary to data protection principles. Consider the imbalance of power between organisations and individuals, and in particular, vulnerable individuals. As an organisation KCC must act responsibly towards the needs not only of wider society but also of the individual. The impact the data sharing would have on individuals' information rights and fundamental human rights require careful thought and balance. Consider any consultation carried out with individuals.
e) Sharing any children's data should be given careful thought and consideration. Data should be shared where it will help to safeguard a child, or promote their mental or physical well-being, or to help identify potential risk. KCC must consider the best interests of the child as part of the compliance with lawfulness, fairness and transparency principle and a high level of privacy should be the default. For more information please refer to the ICO's guidance on sharing information to safeguard children and Working Together to Safeguard Children.

Secure and Protected

Personal data must be secure and protected in transit.

a) Employees are responsible for ensuring KCC's personal data is sent in a secure manner. This will usually be via secure email (having checked the email address is correct). Check guidance on KNet or seek advice if unsure.
b) Where a secure means of transfer is specified, it must be used.
c) Employees sending sensitive and confidential information to external organisations must be trained, competent and understand the importance of confidentiality.
d) Sensitive and confidential information must be sent using a secure method that has been competently risk-assessed or provided for that purpose (e.g.

Outlook 365 or other secure email). Guidance can be found within KCC's Secure Email Policy.

Recipients

Prior to sending personal data, staff must be satisfied that the recipient has adequate data protection measures in place. For regular information sharing, documentation should be in place that provides this assurance. If in doubt, staff must ask their line manager.

When setting up an information sharing arrangement, evidence of the following may be considered adequate:

- Public Service Network Certificate (Public Authorities Only)
- ISO27001 (Information Security Management System) certification or Cyber Essentials Accreditation
- 'Satisfactory' NHS Data Security and Protection Toolkit (Health and Social Care Only)
- Current Kent and Medway Information Sharing Agreement signatory and a Record of Sharing for the agreed purpose
- ICT information risk assessment completed by a competent person
- Screening for and/or a full DPIA completed and checked by the DPO.

Consider and regularly review security measures, both physical and technical in KCC and where appropriate, that of the organisation you are sharing the data with, such as who has access to the data and what access controls are in place for all hardware and software. Consider building and office security and resilience in case of an incident such as a power failure or fire. A DPIA can be an effective means of considering these issues and implementing appropriate mitigation measures.

Internal information sharing

Sharing personal information between services is vital for designing and co-ordinating efficient services that make sense to our customers. When planning to link personal data between services, consider the impact on individual privacy and ensure any proposed processing is lawful and justified.

Only share information that is relevant and proportionate for the purpose. Actively promote the principle of 'data minimisation'.

Data quality must be appropriate for its proposed use. Poor data quality shouldn't be a barrier to release if the recipient understands its limitations.

If a service wants access to personal data collected by another KCC service, it should make a data access request to the data owner stating the purpose.

a) If there is a formal process for access requests, this should be respected.
b) Requests should not be frivolous.

c) If regular extractions are anticipated, the requestor should consider how this may be performed more efficiently (e.g. automated reports or interoperability).

A receiving service must ensure their employees are appropriately trained and understand their responsibilities for confidentiality and security.

Requests for confidential health or adult social care information from KCC's Public Health Intelligence Team should be received positively. The Public Health Intelligence Team has express legal powers to process confidential information within its 'Safe Haven' to meet its statutory obligations. Requests for confidential information must however be pre-approved by KCC's Caldicott Guardian and the sharing must have already been notified to individuals through the service's privacy notice.

Statistical purposes

Further processing (including sharing) for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes are permitted within the UK GDPR, provided that:

- there are additional safeguards in place which ensure that technical and organisational measures are in place to ensure data minimisation.
- the original collection was fair, transparent as to its purpose and lawful, and does not involve special categories (sensitive) or confidential data

Consent is not required for further processing provided that:

- data are not used to support measures or decisions with respect to individuals or where substantial damage or distress is (or is likely to be) caused to any individual,
- resulting products and outputs are not made available in a form that identifies individuals (data subjects).

Processing personal data for the purposes of management forecasting or management planning in relation to a business or other activity are only excepted from the UK GDPR by the Data Protection Act 2018 to the extent that applying the UK GDPR requirements would prejudice the conduct of the business.

IG Library

International Transfers of Data

Personal information should not be transferred to an international organisation or a third country outside the UK without informing individuals of that fact including the names of all countries. In addition, we must confirm that said country or territory ensures an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal information, as determined by the Secretary

of State or where the organisation receiving the personal information has provided adequate safeguards. This is referred to as 'adequacy'.

Did you know: 'Adequacy' is a term the EU uses to describe countries, territories, sectors or organisations it deems to have an "essentially equivalent" level of data protection to the EU. The EU Commission have deemed that the UK GDPR and the Law Enforcement Directive are adequate. This means data can continue to flow freely from the EU to the UK, in most cases. If you are ever unsure, make sure you seek advice before any personal data leaves the UK.

This means that individuals' rights must be enforceable and effective legal remedies for individuals must be available following the transfer. It may also be possible to transfer personal information where the data subject has provided explicit consent or for other limited reasons.

Staff should contact the DPO if they require further assistance with a proposed transfer of personal information; you may need to complete a transfer impact assessment to assess what safeguards can and will be put in place by the company/organisation in the other country.

IG Library

Anonymisation and Pseudonymisation

Where information is shared and the identity of the person serves no purpose or should not be shared, personal data must be anonymised (i.e. identifiers removed so the individual can no longer be re-identified by any means) or pseudonymised (i.e. replaced with an identifier or pseudonym) in accordance with the council's guidance on Anonymisation and Pseudonymisation. Pseudonymised data must be treated in the same way as personal data.

KCC complies with the ICO's Anonymisation Code of Practice in its use of personal data for management information, business intelligence, statistical or research purposes (i.e. secondary purposes). It recognises that anonymisation methods can also be relevant to the safe use or sharing within organisations, particularly large ones with diverse functions.

The Information Commissioner's Office (ICO) stresses the need for organisations to exercise caution when attempting to anonymise personal data. Organisations frequently refer to personal data sets as having been 'anonymised' when, in fact, this is not the case. Any methods used must truly anonymise personal data. There is a clear risk of disregarding the terms of the UK GDPR in the mistaken belief that personal data is not being processed.

Anonymisation

Anonymisation removes all personal information that might identify an individual and irreversibly destroys any way of identifying the individual and is used when organisations do not need access to the personal data. This usually requires removing, obscuring, aggregating, replacing and/or altering any information that might identify an individual and irreversibly destroying any way of re-identifying that individual.

Anonymisation is a process which enables much wider use of information whilst protecting individual privacy and confidentiality. Anonymisation is possible and desirable and ensures the availability of data resources, whilst protecting an individual's personal data. The original identifiable data should be deleted so that the data cannot be re-identified.

To protect the privacy and confidentiality of individuals, personal data should be removed from reports and other outputs where it is not needed or serves no purpose.

Disclosure of 'anonymised' data is not a disclosure of personal data. However, it is not completely risk free and any risk of identification must be mitigated until the risk of re-identification is remote, or negligible.

An effective anonymisation process should consider and document:

- the context and objectives of the anonymisation process
- whether information about someone's private life could end up in the public domain
- if an anonymised database could be 'cracked' so that data about several individuals is compromised
- the likely loss, distress, embarrassment, or anxiety resulting from the re-identification of anonymised data
- the reduced public trust if the council discloses anonymised data unsafely
- the legal problems resulting from the disclosure of insufficiently redacted qualitative data.

It can be difficult to determine whether data has been anonymised or is still personal data; this requires a judgement based on the circumstances. Simply removing or replacing one attribute in a dataset does not prevent someone from identifying an individual e.g. the remaining data may be unusual in combination, or the population size may be small. An indirect identifier (such as gender or date of birth) does identify someone, albeit indirectly, and therefore constitutes personal data under the UK GDPR.

An assessment must be made of all means that a data controller or another person is reasonably likely to use to attempt to re-identify the individuals directly or indirectly. Consideration of this should include objective factors such as the cost and time

required for re-identification, available technology at the time of the processing and technological developments.

There is a range of anonymisation methods and techniques that can be used depending on the data and context:

- Redaction of identifying information from documents
- Blurring of video footage to disguise faces
- Electronically disguising or re-recording audio material
- Changing details in a report.
- Randomisation of a group of techniques used to alter the accuracy of the data by removing the strong link between the data and the individual. (For example, if an individual's height is measured to the nearest centimetre, the dataset is modified to report the individual's height as accurate to only plus or minus 10 to the actual measurement).
- Generalisation or dilution of the attributes of individuals by modifying the scale or magnitude of the data to prevent identification of specific individuals (e.g. presenting combined data on a region rather than a city, using age ranges rather than dates of birth). This can also be referred to as aggregation.
- Removal of recognisable identifiers or variables (characteristics or attributes of an individual) which are direct or indirect identifiers in the dataset. They need not necessarily just be names; a variable should be removed when it is highly identifying in the context of the data.

The robustness of the technique can be assessed considering three criteria:

i. is it still possible to single out an individual,
ii. is it still possible to link records relating to an individual, and
iii. can information be inferred concerning an individual?

The council must ensure that it is not possible to isolate an individual in a data set; link separate data sets concerning the same individual; or deduce, with almost certainty, new information about an individual. A risk assessment should show that the risk of re-identification using reasonable means is zero or negligible.

The council must inform data subjects at the time of collecting personal data (or within one month) that it intends to process data by anonymising it and set out both the purpose and the lawful basis for that processing within its privacy notice(s). This should be included on Privacy Notices.

Any further processing 'for scientific or historical research or for statistical purposes' under Article 9(2)(j) and in accordance with Article 89(1) is not considered to be incompatible with the initial purposes, subject to the following safeguards:

- the anonymisation must not cause substantial damage or substantial distress to particular individuals

- it must not be carried out for the purposes of measures or decisions with respect to particular individuals (unless the necessary purposes are medical research approved by a research ethics committee recognised or established by the Health Research Authority)
- the risks of re-identification are reviewed, monitored and controlled and based on current technologies.

Pseudonymisation

Pseudonymisation is the processing of personal data where the personal data can no longer be attributed to a specific data subject without the use of additional information. Strong pseudonyms are computer-generated and cannot be reversed without a cryptographic key. Where consistently applied, pseudonymisation allows information to be linked in ways that would not otherwise be possible.

To maintain personal data in its pseudonymised state, any additional information that identifies the individual must be kept separate from the pseudonymised data and secure. The level of security should be appropriate to the risk and the additional information or 'key' to the data must be kept separately and securely.

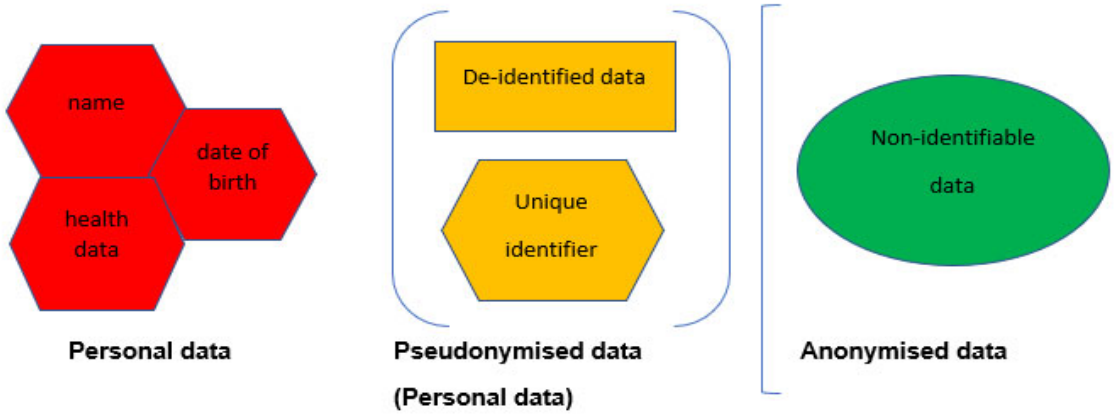
Pseudonymisation is also a measure that implements the data minimisation principle. The UK GDPR recognises that pseudonymisation reduces risks to individuals, but the technique does not exempt data from the UK GDPR (as it does not remove all identifying information from the data but reduces the likelihood of being able to link a dataset with the identity of an individual).

The sharing of pseudonymised data must be documented and managed in the same way as personal data.

Effective pseudonymisation should consider the following:

- each field of personally identifiable information must have a unique pseudonym
- pseudonyms for external use must give different pseudonym values in order that internal pseudonyms are not compromised
- strong pseudonyms replace recognised identifiers such as NHS Number or Unique Pupil Number with a computer-generated identifier
- retaining date of birth and/or postcode may enable re-identification when linked to other available data. Render the data less specific (e.g. use age – range instead of date of birth and Lower Super Output Area instead of postcode)
- pseudonyms should be consistent to preserve data quality
- minimise the number of data items used to those required for the purpose
- handle pseudonymised data as if it were personal data and apply the same protections
- when sharing, do so fairly, transparently and lawfully and apply the same protections as you would for personal data

- do not release pseudonymised data to the public
- to determine whether a natural person is identifiable, take account of all the means reasonably likely to be used, such as singling out, either by the controller or by another person to identify the person directly or indirectly
- to ascertain whether means are reasonably likely to be used to identify the person, take account of all objective factors, such as the costs of, and the amount of time required for, identification, taking into consideration the available technology at the time of the processing and technological developments.



Risk of re-identification

It is essential to carry out a thorough risk analysis on the likelihood and potential consequences of re-identification at the initial stage of producing and disclosing anonymised or pseudonymised data. This includes how other available information might be used to aid re-identification. This is more likely where populations are small or there are unusual features in the data.

A 'motivated intruder' test should be applied to check whether data has been effectively anonymised or pseudonymised. This asks whether a reasonably competent individual could successfully identify individuals from anonymised or pseudonymised data by combining it with online searches or other available information (social networks, online newspapers, press archives, church records, the electoral register or other anonymised data releases) (called a 'jigsaw attack') or where personal knowledge is used to make an educated guess.

Motivated Intruder risk test:

What is the risk – are there characteristics which facilitate linkage – e.g. a code number used in existing published datasets?

What other 'linkable' information is available publicly or easily?

What technical measures might be used to achieve re-identification?

How much weight to be given to personal knowledge?

Consider any re-identification vulnerabilities revealed by a penetration test (detecting and dealing with re-identification vulnerabilities by attempting to re-identify individuals from an anonymised data set using other data available that could be linked).

Re-identification risks associated with others with personal knowledge cannot be ruled out. The likelihood of individuals having and using prior knowledge will need to be assessed. This will be difficult for large datasets so it may be acceptable to make a more general assessment of this risk leading to identification for at least some individuals, and then make a global decision about the information and the chances that those able to do so would come across the data, and what the consequences of re-identification are likely to be for the individual in context. (e.g. disclosure of an address of someone in witness protection would be significant).

It is often difficult to predict the likelihood of re-identification as tools for data analysis and matching become increasingly sophisticated and more readily available, therefore potentially sensitive information should be released with caution and the following guidance applied:

- the risk of re-identification should be assessed or reviewed by a competent person, i.e. someone with sufficient training, knowledge and experience
- sample sizes should be such that deductive assumptions can be avoided
- geographical areas should be aggregated (e.g. Lower Super Output Area) where possible
- restrict circulation and
- document sharing agreements

In borderline cases where the consequences of re-identification could be significant (because they would leave an individual open to damage, distress or financial loss) seek an individual's consent for the disclosure, explaining the possible consequences and adopt a more rigorous form of risk analysis and anonymisation. It should be noted that 'identified' does not necessarily mean 'named' and it can be enough to be able to establish a reliable connection between particular data and a known individual.

Freedom of information

KCC is required to assess whether disclosure in response to a Freedom of Information request would breach data protection laws.

Anonymised information given to a member of the public could be combined with other sources to produce information that identifies an individual. Prior to public release of anonymised information, the risk of re-identification must be assessed, and it should be in a format that prevents re-engineering (e.g. avoid the use of pivot tables) and use csv format spreadsheets.

Open data and transparency rely on the public availability of information, and information released in response to a Freedom of Information Act (FOIA) request cannot be restricted to a particular person or group once it is released.

Disclosure and Publication of Anonymised Data

An individual's properly informed consent is needed for the publication of personal data, unless this is explicitly required by law, therefore it is usually safer to use or disclose anonymised data.

There are very few occasions where personal information would be published (such as member or senior officer remuneration or expenses). The publication of effectively anonymised data is possible provided:

- there are no statutory prohibitions that apply to the disclosure of information that would engage the Freedom of Information Act's section 44 exemption (prohibitions on disclosure in law, contrary to a retained EU obligation or in contempt of court)
- anonymisation has been rigorous, effective and risks to individual privacy considered and documented
- the purpose is legitimate, ethical, and for health and adult social care data, has been approved by the Caldicott Guardian or their delegated support officer
- neither the anonymisation process, nor the use of the anonymised information, will have any direct detrimental effect on any individual
- a privacy notice issued to the data subjects at the time the data is obtained must explain the purpose and the lawful basis for processing the data (and follow the Privacy Notice Guidance) and explain the consequences or rights for individuals
- there is a process for considering complaints from individuals of the use of their anonymised information and a means to object.

Some exemptions from complying with individual rights apply if the council can demonstrate that it cannot identify the individual and informs the individual that is the case.

Different types of anonymised data have different vulnerabilities and pose different levels of re-identification risk. Pseudonymised or de-identified data may be very valuable because of its individual-level granularity and because records from different sources can be easy to match. However, this means there is a high re-identification risk. At the other end of the spectrum, aggregated data is relatively low risk, depending on granularity or sample sizes. In general, the more detailed, linkable and individual level the anonymised data is, the stronger the argument for only limited access to it. The more aggregated and non-linkable the anonymised data is, the more possible it is to publish it. It is therefore important to distinguish between publication to the world at large (e.g. under the FOIA) and limited access

(e.g. within a closed community of researchers) where it is possible to restrict further disclosure or use of the data.

Safeguards for limited access disclosure should include:

- purpose limitation, i.e. the data can only be used by the recipient for an agreed purpose or set of purposes
- training of the recipient's staff with access to data, especially on security and data minimisation principles
- personnel background checks for those getting access to data
- controls over the ability to bring other data into the environment, allowing the risk of re-identification by linkage or association to be managed
- limitation of the use of data to a particular project
- restriction on the disclosure of data
- prohibition on any attempt at re-identification and measures for destruction of any accidentally re-identified personal data
- arrangements for technical and organisational security, e.g. staff confidentiality agreements
- encryption and key management to restrict access to data
- limiting the copying of, or the number of copies of the data
- arrangements for the destruction or return of the data on completion of the project and
- penalties, such as contractual ones that can be imposed on the recipients if they breach the conditions placed on them.

Anonymisation is a heavily context-dependent process and only by considering the data, the environment and the intended use can a well-informed decision be made about what anonymisation is needed. A DPIA will assist in determining whether negligible risk has been achieved and consider the data protection legislation implications (as anonymisation involves processing personal information and if the anonymisation is not carried out correctly, what remains is personal data).

Geo-spatial information

Postcodes and other geographical information may be considered personal data if information about a place or property also provides information about individual(s) who live or work there. The context of related information such as the number of households covered by a postcode must be considered.

When anonymising postcodes, the following average characteristics of postcodes should be considered:

- full postcode = approximately 15 households (beware: some postcodes relate to a single property)
- postcode minus last digit = approximately 120/200 households
- postal sector = first part of the postcode (either 3 or 4 digits) + first digit of second part =approximately 2,600 households

- postal district = first part of the postcode (either 3 or 4 digits) = approximately 8,600 households
- postal area = first two digits of the postcode = approximately 194,000 households

Mobile, smart phones and GDS systems generate significant amounts of detailed spatial information. The council will need to consider how unique identifiers such as IP addresses (personal data) are linked to the spatial information. How information is used by a device or app connected to such devices must be clear to the individual. Risks can be reduced when publishing spatial information by:

- increasing a mapping area to cover more properties or occupants
- reducing the frequency of publication to cover more events
- removing the final 'octet' on IP addresses to degrade the location data they contain
- using formats, such as heat maps, that provide an overview without allowing the inference of detailed information about a particular person or place
- avoiding publication of spatial information on a household level

'Degrading' or 'fading' methods may be useful, exchanging co-ordinates for a ward or city name only.

Key techniques (from the ICO Code of Practice).

Case studies, key methods and other guidance can be found in Annex 2 of the ICO's Anonymisation Code of Practice.

EU guidance describes the most commonly used pseudonymisation techniques:

encryption with a secret key – a two-way algorithm that allows the holder of the key to re-identify each data subject using decryption of the dataset. The encryption key must be protected from disclosure to avoid re-identification.

hash function – a one-way algorithm to change data to another value that cannot be reversed. The data controller may re-identify the personal data by keeping the hash value along with the personal data to map the data. The risk is that the hashing algorithm can be duplicated especially if a third party knows the input values.

keyed hash function with stored key – this corresponds to a particular hash function that uses a secret key as an additional input. The controller can replay the function on the attribute using the secret key, but it is much more difficult for an attacker to replay the function without knowing the key. This method lowers the risk of re-identification because attackers must know potential input values, the hashing algorithm, and the key to re-identify data.

deterministic encryption or keyed-hash function with deletion of the key – This technique involves selecting a random number as a pseudonym for each attribute in the database and then deleting the correspondence table. This diminishes the risk of being able to link the personal data in the dataset with those relating to the same individual in another dataset that uses a different pseudonym. The downside of this technique is that a data controller may not be able to readily re-identify the data and that may limit its use.

tokenization – A technique used to replace card ID numbers by values that have reduced usefulness for an attacker. The token serves as an identifier that traces back to the original data. The tokenization process or related systems must be protected to prevent re-identification.

IG Library

Automated Decision Making

Where KCC carries out automated decision making (including profiling) it must meet all the principles and have a lawful basis for the processing cited in a privacy notice. Explicit consent will usually be required for automated decision making (unless it is authorised by law or it is necessary for the performance of, or entering into, a contract).

Did you know: Data subjects have rights in relation to automated decision making and can ask for the decision to be reviewed. If you are planning a project that involves any automated decisions, you must plan for potential requests and make sure that the rights of individuals are maintained.

Article 22(4) says that you cannot use special category data for solely automated decision-making (including profiling) that has legal or similarly significant effects, unless you have explicit consent or meet the substantial public interest condition. You also need suitable measures in place to safeguard the data subject's rights, freedoms and legitimate interests.

The ICO defines profiling as 'analysing aspects of an individual's personality, behaviour, interests and habits to make predictions or decisions about them'.

Additional safeguards and restrictions apply in the case of solely automated decision-making, including profiling. KCC must, as soon as reasonably possible, notify individuals in writing that a decision has been taken based on solely automated processing and that they may request reconsideration or a new decision. If such a request is received staff must contact the DPO and KCC must reply within 21 days.

IG Library

Freedom of Information

The Freedom of Information Act 2000 (FoIA) establishes a right of access to all types of recorded information held by Public Bodies. It imposes obligations to disclose information through an approved Publication Scheme and in response to requests.

Kent County Council (KCC) will comply with its obligations under the FoIA and will ensure that its staff and customers are aware of their rights under the legislation.

All staff must have a general understanding of the law to be able to make informed judgements about the disclosure and non-disclosure of official information.

The Information Commissioner, as the Regulator, can enforce compliance by taking enforcement action for serious breaches of the Act. It is imperative that KCC complies with our obligations under this legislation.

All KCC staff must ensure they are aware of their responsibilities under the FoIA and KCC's procedures for dealing with requests for information. This will ensure that responses are compliant and are managed within the statutory 20 working day deadline.

All staff must ensure that they are aware of their responsibilities under Section 16 of the Act, to provide advice and assistance, so far as it would be reasonable to expect the authority to do so, to persons who propose to make, or have made, requests for information.

The right of access applies to all recorded information held by KCC or by external parties working on behalf of the Council, regardless of whether the information is owned by the Council.

It applies to information in any recorded format, for example:

- Hard copy - paper records, spreadsheets, minutes, diaries, notebooks etc.
- Electronic information - emails, photographs, videos, mapping data, CDs, etc

Disclosure of requested information is subject to the application of exemptions and where applicable, the application of Public Interest or Prejudice tests. However, it should be remembered that all requests should be approached with an intention of disclosing wherever possible.

IG Library

Environmental Information Regulations

The Environmental Information Regulations 2004 (EIR) establish a right of access to information about the environment held by Public Bodies and other organisations with responsibilities in respect of the environment. The Regulations impose obligations to disclose information through an approved Publication Scheme and in response to requests.

Kent County Council (KCC) will comply with its obligations under the EIR and will ensure that its staff and customers are aware of their rights under the legislation.

All staff must have a general understanding of the law to be able to make informed judgements about the disclosure and non-disclosure of environmental information.

The Information Commissioner, as the Regulator, can enforce compliance by taking enforcement action for serious breaches of the Regulations. It is imperative that KCC complies with our obligation under this legislation.

The Regulations implement the European Union Directive on public access to environmental information and the Directive therefore assists in the interpretation of the Regulations.

The right of access relates to a broad range of environmental information and applies to all recorded environmental information held by KCC or by external parties working on behalf of the Council, regardless of whether the information is owned by the Council.

The Regulations apply to information in any recorded format for example:

- Hard copy - paper records, spreadsheets, minutes, diaries, notebooks etc.
- Electronic information - emails, photographs, videos, mapping data, CDs, etc

Disclosure of information is subject to the application of exceptions and public interest considerations. However, the act communicates a clear expectation that an assumption will always be made in favour of disclosure as much as is possible.

IG Library

Training

KCC offers appropriate training, information, advice and guidance to ensure employees are aware of their personal responsibilities in respect of information security when carrying out their duties.

a) All employees, including temporary and contract, must complete mandatory information governance and data protection training during induction. This is recorded on their HR record (employees) or on Delta (temporary and contract staff). This is accessed through the Delta platform and has been divided into two distinct modules, one that focuses on the UK GDPR specifically and one that encompasses the wider subjects and issues of Information Governance.
b) Information governance training is refreshed every other year. Non-completion is reported to the relevant line manager for action. Persistent non-completion is reported to the appropriate Director and the line manager held accountable for ensuring it is completed.
c) Additional training needs may be identified for specialist roles and professions. These are dealt with in divisional learning and development plans or in individual training plans. For example, colleagues who work within Social Care or who have access to Social Care systems are required to undertake the NHS Data Security Awareness Level 1 module. The course aligns to the new data security standards that came out of the National Data Guardian's review. The course can also be found on Delta and if it is required for your role, it will be triggered as part of the mandatory learning requirement.
d) Senior Information Risk Owner (SIRO), Information Asset Owners and Caldicott Guardian roles must receive specialist training within six weeks of their assignment.
e) KCC will support the DPO by providing the resources necessary to maintain the required standard of expert knowledge.
f) Only trained "appropriately trained professionals/persons/KCC employees" can assess risks to the council's information assets.
g) Training must be recorded on an individual's employee record and be available in a way that allows corporate and regulatory oversight (i.e. the ability to produce aggregated reports and statistics and on demand by the ICO).
h) It is the responsibility of line managers to ensure employees moving or changing roles are made aware of local operating procedures.

Other non-mandatory courses can be found on Delta that are recommended depending on your role at KCC or your areas of interest, such as Records Management and an introduction to Freedom of Information.

IG Library

Glossary

Accuracy: is a principle under the UK GDPR that personal data must be accurate and kept up-to-date and corrected or deleted without delay when inaccurate

Aggregation: presents statistical data as combined totals showing trends or values without identifying individuals. Small numbers in totals are a risk and may need to be omitted or 'blurred' through random addition and subtraction.

Anonymisation: is the process of transforming identifiable personal information into non identifiable (anonymous) information. This usually requires removing, obscuring, aggregating, replacing and/or altering any information that might identify an individual and irreversibly destroying any way of re-identifying that individual.

Automated Decision-Making (ADM): when a decision is made which is based solely on Automated Processing (including profiling) which produces legal effects or significantly affects an individual. The UK GDPR prohibits Automated Decision-Making (unless certain conditions are met) but not Automated Processing.

Automated Processing: any form of automated processing of Personal Data consisting of the use of Personal Data to evaluate certain personal aspects relating to an individual, in particular to analyse or predict aspects concerning that individual's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements. Profiling is an example of Automated Processing.

Combining Data: Where data already exists, it is important to ensure that the data is still being used in line with its original purpose. Even if some of the data is collected specifically for the activity, combining it with existing data may increase the risk. An important consideration is whether the individual would reasonably expect the operation to take place and if they may object.

Consent: agreement which must be freely given, specific, informed and be an unambiguous indication of the Data Subject's wishes by which they, by a statement or by a clear positive action, signifies agreement to the Processing of Personal Data relating to them.

Criminal Offence data: Criminal offence data is personal data relating to criminal convictions and offences, or related security measures. This includes data relating to the alleged commission of offences by the data subject, or proceedings for an offence committed or alleged to have been committed by the data subject or the disposal of such proceedings, including sentencing.

Data: information that takes many forms and includes information printed or written on paper (including photocopies and faxes), stored electronically (e.g. on computers or networked storage, disk media, digital tape, memory cards or sticks), transmitted

by post or using electronic means, images, stored negatives, prints, slides, tape or video, spoken in conversation or via telephone.

Data Controller: means the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of Personal Data. It is responsible for establishing practices and policies in line with the UK GDPR. Kent County Council is the Data Controller of all personal information relating to its clients, customers and staff.

Data intruder: a data user who attempts to disclose information about an individual through identification and/or attribution (by association with a particular data population unit (person, household etc). Intruders may be motivated intruders or inadvertent intruders. Motivated intruders may wish to discredit or harm the data controller or profit. Inadvertent intruders may spontaneously recognise individual cases within a dataset.

Data minimisation: a principle under the UK GDPR that personal data should be adequate, relevant and limited to what is necessary for the purpose of the processing.

Data Processor: A data processor is a natural or legal person, public authority, agency or other body which processes personal data on behalf of the data controller. A data processor processes personal data only on the instructions of the data controller.

Data Protection by Design: implementing appropriate technical and organisational measures in an effective manner to ensure compliance with the UK GDPR such that necessary safeguards are integrated into the processing from the outset.

Data Protection Impact Assessment (DPIA): tools and assessments used to identify and reduce risks of a data processing activity. DPIAs can be carried out as part of Data Protection by Design and should be conducted for all major systems or business change programs involving the processing of Personal Data.

Data Protection Officer (DPO): the person required to be appointed in public authorities under the UK GDPR.

Data Subject: a living, identified or identifiable individual about whom KCC holds Personal Data. Data Subjects may be nationals or residents of any country and may have legal rights regarding their Personal Data.

Disclosure: The act of making data available to one or more third parties.

EEA: the 28 countries in the EU, and Iceland, Liechtenstein and Norway.

Explicit Consent: consent which requires a very clear and specific statement (that is, not just action).

General Data Protection Regulation (GDPR): the General Data Protection Regulation ((EU) 2016/679). Personal Data processed in the EU by a data controller based in the UK is subject to the legal safeguards specified in the GDPR.

Identifier: A feature which can identify an individual. Direct identifiers are any attributes or combination of attributes that are unique such as unique reference numbers (e.g., name, address, NHS number). Indirect identifiers can be any attributes or a combination of attributes that are likely to be unique for individuals in a dataset (e.g., it might be a combination of age, marital status and location variables such as a 16-year-old widower living in a particular rural postcode will almost certainly be unique relative to other combinations (e.g. a single person in their 40s living in London).

Innovative technologies: Innovative technology concerns new developments in technological knowledge in the world at large, rather than technology that is new to you, and its use can trigger the need to carry out a DPIA. The personal and social consequences of deploying a new technology might not be known and a DPIA will help you to understand risks. It may also include implementing existing technology in a new way.

Integrity and confidentiality: a principle under the UK GDPR that personal data is secured by appropriate technical and organizational measures against unauthorized or unlawful processing and against accidental loss, destruction, or damage.

Invisible processing: This is where you obtain personal data about an individual from another source and not directly from the individual, and you do not provide the individual with privacy information as required by Article 14 UK GDPR. The individual is therefore unaware their personal data is being collected and used by you. UK GDPR only permits 'invisible processing' where providing privacy information would prove impossible (for example, there are no contact details for the individuals and there are no reasonable means of obtaining them) or involve disproportionate effort. You must be able to justify any reliance on the disproportionate exception, and take other measures to protect individuals' rights, for example, still publishing privacy information on KCC's website and carrying out a DPIA. This will help to assess whether you are taking a proportionate approach and what other measures could be taken to support the exercise of individuals' rights.

Joint Data Controllers: Where two or more data controllers jointly determine the purposes and means of the processing of the same personal data for the same or shared purposes. They will not be joint data controllers if they are processing the same personal data but for different purposes.

Large scale processing: When determining the scale of the activity you should consider four factors:

- The number of data subjects concerned – consider this alongside the relevant population and the proportion affected by the processing. E.g. the population of Kent, a district, a demographic group or service users.
- The volume and/or range of data used – consider if all the data is from a single category, e.g. finance, and how much detail is required.
- The duration of the activity – some processing activities have a clear end whereas others would be continuous.
- The geographic extent of the activity – consider where the activity takes place, local, regional, national etc.

There is no set measure of large scale but any one of these factors could trigger high risks to data subjects. You may wish to document the justification for judgements made about the scale of processing operations.

Some examples given by the ICO include:

- a hospital (not an individual doctor) processing patient data
- tracking individuals using a city's public transport system
- a fast-food chain tracking real-time location of its customers
- an insurance company or bank processing customer data
- a search engine processing data for behavioural advertising
- a telephone or internet service provider processing user data.

Lost and Stolen: applies to hard copy information as well as computerised equipment, e.g. file left in a vehicle or on public transport or stolen with car or snatched in a bag, etc. Also applies to any personal details or sensitive information passed to an unauthorised individual in any manner or overheard by an unauthorised individual during a conversation.

Loss: In the event of the item being knowingly lost as opposed to stolen, all of the above applies except that the Police will not report a crime and cannot issue a crime number.

Malicious: Giving information to someone who should not have access to it – verbally, in writing or electronically, computer infected by a virus or similar, sending a sensitive email to the wrong recipient, receiving unsolicited mail of an offensive nature, finding data that has been changed by an unauthorised person, receiving and forwarding chain letters, including virus warnings, scam warnings and other emails which encourage the recipient to forward to others, unknown people asking for information which could gain them access to data e.g. a password or information about a third party

Misuse: Use of unapproved or unlicensed software on KCC equipment, accessing a computer database using someone else's authorisation (e.g. user ID/password), writing down your password and leaving it on display or printing or copying confidential information and not storing it correctly or confidentially

‘Motivated Intruder’ Test: involves determining whether a ‘motivated intruder’ (a person who starts without any prior knowledge but wishes to identify the individual from whose personal data the anonymized data has been derived), would be successful. It can be done by:

i. carrying out a web search to verify if date of birth and postcode can lead to the identification of a specific individual; or
ii. (ii) using social networks to establish if anonymized data can lead to an individual’s profile.

Personal Data: is any information relating to an identified or identifiable natural person (‘data subject’) who can be identified, directly or indirectly by reference to an identifier such as a name, identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

Personal Data Breach: means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed.

Primary use: refers to identifying personal information used to deliver social care or health care to individuals. This information would directly contribute to the treatment, diagnosis or the care of the individual and includes relevant supporting administrative and service management processes and audits of the quality of the service provided.

Privacy Notices: separate notices setting out information that may be provided to Data Subjects when KCC collects information about them. These notices may take the form of general privacy statements applicable to a specific group of individuals (for example, employee privacy notices or the website privacy policy) or they may be stand-alone, one-time privacy statements covering processing related to a specific purpose.

Processing: means anything done with personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

Processor: means a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller.

Profiling: Profiling is an automated process which evaluates individuals based on certain personal data. Information commonly used for this purpose includes performance at work, economic situation, health, personal interests, and behaviour or location. The production of a score or rating based on personal data is a good indication that profiling has taken place. Even if profiling has not taken place, any

activity that results in a prediction should be considered a risk. E.g. banks screening customers against an existing credit reference database. A local authority decision that could lead to changes in service provision could significantly affect individuals.

Pseudonymisation: means processing personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information provided that such additional information is kept separately and is subject to technical and organisational measures to ensure that the personal data are not attributed to an identified or identifiable natural person.

Purpose Limitation: a principle under the UK GDPR that personal data should only be collected for specified, explicit and legitimate purposes and should not be processed in an incompatible manner with those purposes, except under limited circumstances.

Qualitative data: Data gathered and analysed in a non-numeric form, such as interview transcripts, video and audio recordings, meeting minutes, e-mails.

Re-identification or de-anonymisation: where anonymised data is turned back into personal data using data matching or combining. The anonymisation process must be designed to minimise the risk of re-identification so that the chances are remote or negligible.

Secondary use: information about individuals for non-care or research purposes. This includes population health surveillance, commissioning, evaluation and contract management. When data derived from personal identifiable data are required for secondary uses, this should be limited and de-identified so that the process does not identify individuals.

Security Incident: awareness of the possibility or actuality of a breach of security. This can take many forms, e.g. unauthorised access to, or the loss or theft of, KCC computerised equipment; the mislaying of a client's manual case file or the inappropriate disclosure of information (verbally, in writing or electronically) to someone who has no right or need to access it.

Significantly affect: In the context of profiling, this means it will have a noticeable impact on an individual and can significantly affect their circumstances, behaviour or choices. A legal effect is something that affects a person's legal status or legal rights. A similarly significant effect might include something that affects an individual's financial status, health, reputation, access to services or other economic or social opportunities.

Special Categories of Personal Data: information revealing racial or ethnic origin, political opinions, religious or philosophical beliefs or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation.

Statistical data: Information held in the form of numerical data, nominal data (e.g. gender, ethnicity, religion), ordinal data (age group, qualification level), interval data (month of birth) or ratio data (age in months).

Storage limitation: a principle under the UK GDPR which requires that personal data is kept in identifiable form only for as long as necessary to fulfil the purposes the organisation collected it for, subject to limited exceptions.

Systematic and extensive: 'Systematic' means that the processing:

- occurs according to a system
- is pre-arranged, organised or methodical
- takes place as part of a general plan for data collection or
- is carried out as part of a strategy.

'Extensive' implies the processing also covers a large area, involves a wide range of data or affects a large number of individuals.

Theft/loss: Theft/loss of a hard copy file or theft/loss of KCC computer equipment

United Kingdom General Data Protection Regulation ('UK GDPR'): Regulation EU 2016/679 https://op.europa.eu/en/publication-detail/-/publication/3e485e15-11bd-11e6-ba9a-01aa75ed71a1/language-en as it forms part of UK law by virtue of section 3 of the European Union (Withdrawal) Act 2018 as confirmed in The Data Protection, Privacy and Electronic Communications (Amendments etc) (EU Exit) Regulations 2019.

Vulnerable individuals: Using the personal data of vulnerable people increases the risk of a power imbalance between KCC and the data subject. Vulnerability should be judged according to the context of an individual's ability to oppose, prevent or understand the processing. For example, children and vulnerable adults. Employees should also be classed as vulnerable in the context of their employer.

Footnotes

KCC supports the principles outlined in the Code of Recommended Practice for Local Authorities on Data Transparency (2015) and commits to:

a. consider the release of datasets in response to public demand
b. publish data in open and machine-readable formats where reasonable
c. publish data and information in a timely manner.

KCC complies with the Freedom of Information Act 2000 and Environmental Information Regulations 2004, and is committed to:

a. handling requests in a courteous and helpful manner and responding within the prescribed time limit

b. operating a publication scheme that shows what information is routinely published.

KCC supports the principles outlined in the Lord Chancellor's Code of Practice on the Management of Records and maintains policies and procedures for monitoring the quality of records management.

Employees who manage contracts are responsible for ensuring that contractors comply with their obligations in relation to the confidentiality and security of personal data and include the specific terms required by the UK GDPR.

Procedures and arrangements are in place to manage communications with the public, press and broadcast media.

If staff, suppliers or Members do not understand this guidance, or if more details are needed regarding any of the steps or staff and others' responsibilities, then contact KCC's:

- Divisional Information Governance leads
- Information Resilience and Transparency Team: dataprotection@kent.gov.uk
- Data Protection Officer: DPO@kent.gov.uk
- Advice on Information Security and Information Risk Management can be obtained by contacting the ICT Compliance and Risk Team ictcomplianceandrisk@kent.gov.uk

Related Policies

This policy should be used in conjunction with the following related policies:

- Open Data Policy
- Digital Continuity Policy
- Kent and Medway Information Sharing Agreement
- ICT Security Standard
- Electronic Communications Policy
- Malicious Software Protection Policy
- Artificial Intelligence Policy

IG Library