Adult Social Care and Health (ASCH) Directorate

Business Delivery Unit: Information Governance

Appropriate Policy Document

Document details

Issue Date:	May 2022
Review Date:	May (every year)
Contact Details:	Systems & Performance (Business Delivery Unit) 3rd Floor Invicta House Maidstone Kent ME141XX
Owner:	Lauren Liddell-Young Lauren.liddell-young@kent.gov.uk 03000 414424

Version control (record of summary changes to document)

Date	Changed by	Page/ paragrap	Summary of change
May 2019	Janice Grant	Whole document	First published appropriate policy for lawful processing
March 2022	Lauren Liddell-Young	Whole document	Updates made to reflect operational practice and requirements and feedback from DPO Team

Contents

Introduction

This guidance is the Appropriate Policy Document for ASCH staff to use when processing personal and special category data and/or criminal convictions or offences data to ensure this processing is lawful.

The Appropriate Policy Document is required under UK GDPR, Section 39 in Part 4 of Schedule 1 where the following conditions are relied upon:

- Employment, social security, and social protection (condition in Part 1 Section 1).
- Any of the substantial public interests conditions (conditions in Part 2 Sections 6-28).
- Any of the specific conditions in Part 3 relating to criminal offence data (Section 35: administration accounts used in commission of indecency offences involving children. Section 36: extension of conditions in Part 2 referring to substantial public interest).

This guidance should be referenced alongside KCC policies and ASCH policies where these involve the processing of personal data.

Scope

This document relates to the lawful processing of personal data regarding direct care being provided to individuals.

Personal data only includes information relating to natural persons who:

- can be identified or who are identifiable, directly from the information in question; or
- who can be indirectly identified from that information in combination with other information.

Pseudonymised data can help reduce privacy risks by making it more difficult to identify individuals, but it is still personal data.

Special category data is personal data that is classed as more sensitive, and this data can only be processed in more limited circumstances. Special category data is defined as being:

- 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
- data concerning a person’s sexual orientation.

Special category data does not include personal data about criminal allegations, proceedings or convictions as separate rules apply. To process criminal allegations, proceedings or convictions, you must identify a lawful basis under Article 6 and either an official authority or a Schedule 1 condition under Article 10.

Special category data is personal data that the GDPR says is more sensitive, and so needs more protection. To lawfully process special category data, you must identify both a lawful basis under Article 6 and Article 9 plus a separate condition for processing from the Data Protection Act 2018 (DPA) where necessary.

Lawful Basis

To lawfully process personal data, you must have identified an appropriate lawful basis under Article 6(1). The lawful bases selected must be the most suitable and relevant to your intended processing.

There are 6 lawful bases in total, but the following are the most suitable and relevant to processing for ASCH.

(b) Contract: the processing is necessary for a contract you have with the individual, or because they have asked you to take specific steps before entering into a contract.

(c) Legal obligation: the processing is necessary for you to comply with the law (not including contractual obligations).

(e) Public task: the processing is necessary for you to perform a task in the public interest or for your official functions, and the task or function has a clear basis in law.

Conditions for Processing Special Category Data

To lawfully process special category data, in addition to identifying a lawful basis under Article 6, an Article 9(2) condition needs to be identified. As when selecting the lawful bases, this must be the most suitable and relevant to your intended processing.

There are 10 conditions for processing special category data in total, but the following are the most suitable and relevant to processing for ASCH.

(g) Substantial public interest: processing is necessary for reasons of substantial public interest, on the basis of Union or Member State law which shall be proportionate to the aim pursued, respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject.

- If Article 9(2)(g) condition above is relied on, you will also need to meet one of the 23 specific substantial public interest conditions. These are set out in Schedule 1 of the DPA 2018 (at paragraphs 6 to 28). You must also have an Appropriate Policy Document in place for almost all of these conditions.
- Examples whereby ASCH duties or functions undertaken that apply could be:
    - **Equality of Opportunity or Treatment**
        - This condition is met if the processing is (a) is of a specified category of personal data, and
        - (b), necessary for the purposes of identifying or keeping under review the existence or absence of equality of opportunity of treatment between groups of people specified in relation to that category with a view to enabling such equality to be promoted or maintained. Subject to the exceptions in sub-paragraphs (3) to (5).

- Processing does not meet the condition in sub-paragraph (1) if it carried out for the purposes of measures or decisions with respect to a particular data subject.
- Processing does not meet the condition in sub-paragraph (2) it is likely to cause substantial damage or substantial distress to an individual.
- Processing does not meet the condition in sub-paragraph (1) if (a) an individual who is the data subject (or one of the data subjects) has given notice in writing to the controller requiring the controller not to process personal data in respect of which the individual is the data subject (and has not given notice in writing withdrawing that requirement), (b) the notice gave the controller a reasonable period in which to stop processing such data, and, (c) the period has ended.

    - Equalities monitoring data could be used as part of an Equalities Impact Assessment for example. This may be collected at the same time as personal data. Examples of this type of data include personal data revealing racial or ethnic origin, religious of philosophical beliefs, data concerning health, personal data concerning an individuals' sexual orientation.
    - Equalities monitoring data is a choice and the data subject may prefer not to share it.
    - Where possible/applicable, equalities data should be anonymised or pseudonymised to help ASCH remain compliant with data security and minimisation.

- **Safeguarding of children and individuals at risk**
    - This condition is met if the processing is (a) necessary for the purpose of (i) protecting an individual from neglect or physical, mental or emotional harm, (ii) protecting the physical mental or emotional wellbeing of an individual,
    - The individual is (i) aged under 18, or, (ii) aged 18 or over and at risk,
    - The processing is carried out (c) without the consent of the data subject for one of the reasons listed in sub-paragraph (2), and (d), the processing is necessary for substantial public interest.
    - The reasons mentioned in sub-paragraph 1(c) are (a) in the circumstances, consent to the processing cannot be given by the data subject, (b) in the circumstances, the controller cannot reasonably be expected to the consent of the data subject for processing, (c) the processing must be carried out without the consent of the data subject because obtaining the consent of the data subject would prejudice the provision of the protection mentioned in sub-paragraph (1)(a).
    - For the purposes of this paragraph, an individual aged 18 or over is "at risk" if the controller has reasonable cause to suspect that the individual, (a)has needs for care and support, (b) is experiencing, or at risk of, neglect or physical, mental or emotional harm, and (c)as a result of those needs is unable to protect himself or herself against the neglect or harm or the risk of it.
    - In sub-paragraph (1)(a), the reference to the protection of an individual or of the well-being of an individual includes both protection relating to a particular individual and protection relating to a type of individual.

        - When processing children's data for this purpose, the best interests of the child shall be a primary consideration.
        - When processing adult's data for this purpose, it needs to be on a 'need to know' basis.
        - The Children's Act 1989 and 2004 and The Care Act 2014 reinforce functions, duties etc. that Local Authorities need to undertake.

(h) Provision of Health or Social Care: processing is necessary for the purposes of preventive or occupational medicine, for the assessment of the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment or the management of health or social care systems and services on the basis of Union or Member State law or pursuant to contract with a health professional and subject to the conditions and safeguards referred to in paragraph 3.

- If Article 9(2)(h) condition above is relied on, you will also need to meet the associated condition in UK Law. This is set out in Part 1 Schedule 1 of the DPA 2018.
    - If the health or social care purposes condition is selected, this need to be either (a) under a health professional or a social work professional; or (b) another person who in the circumstances owes a duty of confidentiality under an enactment or rule of law.
- Examples whereby ASCH duties or functions undertaken that apply could be:
    - Direct care or administrative purposes.

Conditions for Processing Criminal Allegations, Proceedings or Convictions

To process criminal allegations, proceedings or convictions, in additional to a lawful basis under Article 6, you must identify either an official authority or a Schedule 1 condition under Article 10. As when selecting the lawful bases, this must be the most suitable and relevant to your intended processing.

Under the control of official authority means that public bodies may have 'official authority' laid down by law to process criminal offence data. This may derive from either common law or statute. A public body is responsible for identifying the specific law. Sufficient official authority is also required if you wish to keep a comprehensive register of criminal convictions.

If you cannot rely on 'official authority', processing criminal allegations, proceedings or convictions information must be authorised by domestic law. In the UK, the authorisation in law is set out in the Schedule 1 conditions listed in the DPA 2018. There are 28 conditions to process criminal offence data, but the following are the most suitable and relevant to processing for ASCH:

- (2) health or social care purposes
- (6) statutory and government purposes
- (10) preventing or detecting unlawful acts
- (18) safeguarding of children and individuals at risk
- (29) consent
- (30) vital interests

Detailed provisions of each condition can be found on legislation.gov.uk.

How ASCH complies with UK GDPR Data Protection Principles

UK GDPR (Article 5) has six data protection principles that a data controller must abide by. Kent County Council is responsible for ensuring these are followed when processing personal data and must be able to demonstrate compliance.

Principle 1

The principle is (1)(a) processed lawfully, fairly and in a transparent manner in relation to individuals (lawful, fairness and transparency).

ASCH will:

- Ensure processing personal information will only take place when appropriate lawful bases have been identified. The same also applies to processing special category information under Article 9 and criminal allegation, proceeding or convictions information under Article 10.
- Ensure privacy notices have been supplied to individuals we support, their families and support networks where applicable, unless this proves impossible or would involve a disproportionate effort. Privacy notices ensure transparency and informs individuals how their personal data will be collected and processed. ASCH privacy notices can be found on kent.gov and are split into a General Notice and specific services.
- Individuals being supported (and their families and/or support networks) are treated fairly, without discrimination, prejudice, or judgement.
- Ensure that practitioners understand their professional obligation of confidentiality under the 'Common Law Duty of Confidentiality.
    - The Common Law Duty of Confidentiality refers to an individual's personal data being disclosed where there is a legal authority or justification to do so. There needs to be lawful basis for this disclosure to take place. The lawful bases include:
        - Where the individual has capacity and has given valid informed consent
        - Where the disclosure is in the overriding public interest
        - Where there is a statutory basis or legal duty to disclose e.g., by court order.
    - The Health and Social Care Act 2012 (section 251B) gives a statutory duty to health and social care providers to share information about a patient (individual) for their direct care. This duty is subject to the common law duty of confidentiality and DPA 2018 and UK GDPR.

Principle 2

The principle is (1)(b) collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall not be considered to be incompatible with the initial purposes (purpose limitation).

ASCH will:

- Only collect personal data for specified, explicit and legitimate purposes.
- Inform data subjects for what those purposes are in a privacy notice. ASCH privacy notices are available on KCC's website.
- Not use personal data for purposes that are incompatible with the purposes for which it was collected. If personal data is used a purpose that is new, different, or incompatible, we will inform the data subject of the new purpose and seek their consent where necessary.

Principle 3

The principle is (1)(c) adequate, relevant, and limited to what is necessary in relation to the purposes for which they are processed (data minimisation).

ASCH will:

- Ensure that only the minimum amount of personal data for the purpose for which it is collected. Personal data collected will also be adequate and relevant.
- Ensure staff only process personal information for when their role requires it. Information unrelating to their role will not be processed.
- Data must be recorded in-line with ASCH policies e.g., Case Recording Policy. This Policy sets out six standards that align very closely to the data protection principles

Principle 4

The principle (1)(d) accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay (accuracy).

ASCH will:

- Ensure that personal information is accurate and kept up to date where necessary.
- Ensure that requests to update information are upheld to ensure accuracy of personal information. This includes taking reasonable steps to ensure that personal data is erased or rectified without delay. If inaccuracies cannot be corrected, a note will be recorded on a case record to reflect the viewpoint on the individual.
- Take particular care to do this where our use of the personal data may have a significant impact on individuals.
- Data will be recorded in-line with ASCH policies e.g., Case Recording Policy.
- Data quality concerns and issues are addressed through ASCH's Data Quality Strategy which focuses on improving the six characteristics of data quality: (a) the accuracy of data, (b) the validity of data, (c) the reliability of data, (d), the timeliness of data, (e) the completeness of data and (f) the availability of data.

Principle 5

The principle (1)(e) kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal

data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes subject to implementation of the appropriate technical and organisational measures required by the GDPR in order to safeguard the rights and freedoms of individuals (storage limitation).

ASCH will:

- Only keep personal data in identifiable form as long as necessary for the purposes for which it is collected, or where it has a legal obligation to do so. Once no longer required personal data will be deleted or disposed of in-line with KCC's Retention Schedule or made permanently anonymous.

Personal data will be deleted in accordance with the Retention Schedule (and Information Management Manual) which lists all retention periods applicable to ASCH. These are AS1-6 and exclude: AS2.1, AS2.2, AS4.4, AS4.5, AS4.9, AS4.10, AS4.11, AS4.12.15, AS4.12.16, AS4.13, AS5.2, AS6.1). The Retention Schedule ensures that ASCH only keep information for a reasonable time to account for statutory or industry requirements, legal liability or other legal requirements and best business practice.

ASCH also maintains a Record of Processing Activity (ROPA) to demonstrate where, how and why data is being pressed and under what legal basis.

Principle 6

The principle is (1)(f) processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction, or damage, using appropriate technical or organisational measures ('integrity and confidentiality (integrity and confidentiality).

ASCH will:

- Use appropriate technical and organisational measures in accordance with KCC policies to keep personal information secure, and in particular, to protect against unauthorised or unlawful processing against accidental lost, destruction or damage.
- Develop, implement, and maintain safeguards appropriate and necessary and proportionate to the size, scope, business, available resources, and the amount of personal information that is owns or maintains on behalf of others and identified risks (including the use of encryption and pseudonymisation where applicable and in accordance with KCC's Anonymisation and Pseudonymisation Policy). It will regularly evaluate and test the effectiveness of those safeguards to ensure security of processing.
- Ensure that when processing any personal information, it is done in an authorised manner and subject to a duty of confidentiality, with integrity and resilience.
- Ensure that when sharing information with third parties, those receiving the personal data also have adequate measures in place to protect that data.
- When using 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.

- Staff to report, within 4 hours of becoming aware, any breach or suspect breach to the Information Resilience and Transparency Team.
- Ensure that data is stored securely, password protected where suitable and accessible only by those who have a legitimate need to process it. This is explained in more detail in the Case Recording Policy.

ASCH staff are required to undertake KCC's mandatory training on Introduction to Information Governance and GDPR: Data Protection Essentials every two years and NHS Data Security Awareness Level 1 every year.

Duty of Confidence

The Common Law Duty of Confidentiality refers to common law that has been developed through the courts. It makes decisions in cases on legal points and creating binding precedents. Disclosure may only be justified in one of three ways:

- the service user has given consent for their information to be used
- the balance of public and private interest favours public interest disclosure; or
- a statutory basis exists which permits or requires disclosure.

This can include statutory purposes relied on for health or social care organisations.

Accountability

The following roles and responsibilities in KCC are:

- Data Protection Officer (DPO) who is required to monitor internal compliance, to inform and advise on data protection obligations, provide advice on DPIAs and act as a contact point for data subjects and the supervisory authority.
- Senior Information Risk Owner (SIRO) who is concerned with the management of all information assets, fosters a culture for protecting and using data and providers a focal point for managing information risks and incidents.
- Caldicott Guardian who is the conscience of the organisation, is concerned with the management of client information and provides a focal point for client confidentiality and information sharing issues.

The following roles and responsibilities in ASC are:

- Information Governance (IG) Lead who provides support and assistance on queries or concerns and is a single point of contact for any queries.
- Caldicott Guardian Support Officer (CGSO) who provides support to the Caldicott Guardian and advises on compliance with the Caldicott Guardian principles.

The Information Governance Management Framework sets out Kent County Council's (KCC) management arrangements for ensuring personal information is handled securely and effectively, and in compliance with its legal and regulatory obligations.

As a Data Controller, KCC is responsible for:

- Ensuring staff are aware of data protection obligations under UK GDPR/DPA 2018 and follow guidance and legislation.
- Ensuring data subjects are informed on how their information will be collected and used by ASCH. This can be in the form of a privacy notice.
- Carrying out Data Protection Impact Assessment where any processing is likely to result in a high risk to the rights and freedoms of individuals.
- Embedding privacy by design principles e.g., organisational, and technical measures effectively to ensure compliance with data privacy principles e.g., minimisation.
- Ensuring the Records of Processing Activities is kept up to date for any processing of personal data. For ASCH staff please contact lauren.liddell-young@kent.gov.uk (Information Governance Lead).

Review Period

This document will be reviewed on a yearly basis (May). Any changes or updates will be reflected within the version control and circulated thereafter as soon as possible.

Please email lauren.liddell-young@kent.gov.uk regarding any updates or changes for this document.

Useful Links

This document should be used in conjunction with KCC Policies and Procedures available on Knet that are relevant to processing personal (and sensitive) data.

The Information Commissioners Office website provides a breakdown of information on UK GDPR.