Data Protection & Confidentiality Policy

December 2020

This policy provides the framework to ensure that the Council complies with the requirements of the General Data Protection Regulation, The Data Protection Act 2018, the Caldicott Principles for handling personal confidential data and the Common Law duty of Confidentiality.

Summary Sheet

Document Information

Protective marking (Unclassified / Restricted Circulation / Confidential)	Unclassified
Ref	IG Policy 4
Document purpose	Council obligations under data protection legislation
Document status (Draft / Active)	Draft
Partners (If applicable)	N/A
Date document came into force	25th May 2018
Date of next review	Twelve-month basis as part of Annual Information Governance statement taken to Information Management Executive Group
Owner (Service Area)	Sefton Council – Performance & Business Intelligence Service
Location of original (Owner job title / contact details)	Catherine Larkin (Information Management and Governance Lead – DPO)
Authorised by (Committee/Cabinet)	Information Management Executive Group (08/07/2020) Audit & Governance Committee (insert date)

Document History

Version	Date	Author	Notes on revisions
1.0	January 2014	Ben Heal (DPO).	Initial Draft.
2.0	April 2014	Ben Heal (DPO).	Amendments following consultation
3.1	November 2014	Ben Heal DPO who revised document purchased from Act Now IG consultancy.	On ICO advice to be taken to full Cabinet for ratification.
4.0	May 2018	Wayne Leatherbarrow	The document has been amended to reflect that the Data Protection Act (DPA) 1998 has been repealed, and the new General Data Protection Regulation (GDPR) comes into force on the 25th May 2018.
5.0	August 2019	Catherine Larkin (DPO)	Revisions following annual review

Contents

1 Summary

Data Protection and confidentiality are legal requirements on all staff working in the Council.

The UK data protection regime is set out in the DPA 2018 along with the GDPR which also forms part of UK law.

The GDPR is the General Data Protection Regulation (EU) 2016/679. It sets out the key principles, rights and obligations for most processing of personal data – but it does not apply to processing for law enforcement purposes, or to areas outside EU law such as national security or defence.

The GDPR came into effect on 25 May 2018. As a European Regulation, it has direct effect in UK law and automatically applies in the UK until we leave the EU (or until the end of any agreed transition period, if we leave with a deal). After this date, it will form part of UK law under the European Union (Withdrawal) Act 2018, with some technical changes to make it work effectively in a UK context.

The DPA 2018 is split into a number of different parts, which apply in different situations and perform different functions. It sets out four separate data protection regimes:

- Part 2 Chapter 2: General processing (GDPR);
- Part 2 Chapter 3: General processing (applied GDPR);
- Part 3: Law enforcement processing; and
- Part 4: Intelligence services processing

Data protection law is regulated by the Information Commissioner's Office (ICO). They are the UK's 'supervisory authority'. Their role is to offer advice and guidance, promote good practice, carry out audits and advisory visits, consider complaints, monitor compliance and take enforcement action where appropriate.

Enforcement action may take the form of issuing information notices that require us to provide the ICO with certain information. The Information Commissioner can instruct us to take specific steps or actions or stop us from taking certain actions. They have powers of entry and inspection and have the right to issue civil monetary penalty notices in cases of serious infringements of the legislation. The maximum amount is €20 million (or equivalent in sterling) or 4% of the total annual worldwide turnover of an organisation, whichever is higher.

There are a number of criminal offences under the DPA 2018. These include:

- Unlawful obtaining of personal data
- Re-identification of de-identified personal data
- Alteration of personal data to prevent disclosure to a data subject

.

Data protection is concerned with respecting the rights of individuals when processing their personal information. This can be achieved by being open and honest with employees and citizens about the use of information about them and by following good data handling procedures. All organisations that hold or process personal data must comply with the DPA 2018 and the GDPR.

Data protection is not a barrier to justified processing and sharing information, if a defined "legal basis" has been identified and recorded. The legislation also sets out some 'exemptions' where the Council as the data controller need not comply with all the usual rights and obligations. There are number of these exemptions, which are explained later in this document.

All staff must complete annual Information Governance Training, which covers Data Protection and Confidentiality.

Staff must not access any records which constitute personal data unless they are authorised to do so. Any individuals found to have unauthorised access to personal data could face disciplinary action and it may ultimately lead to prosecution by the Information Commissioner's Office. Staff must not access records relating to family members or friends, even if they are asked to do so by those individuals. If you have concerns about how this may affect you, you must raise your concern at the earliest opportunity with your Line Manager and the Council's Data Protection Officer.

If staff require advice or support on any Data Protection or confidentiality matter, they should contact their information Asset Owner IAO) in the first instance http://intranet.smbc.loc/our-council/data-handling-foi/information-asset-owners.aspx , who may escalate the issue to either the Council's Data Protection Officer or Caldicott Guardian.

2 Introduction

This document describes the Council's (Sefton Council) policy on **Data Protection** (General Data Protection Regulation and DPA 2018); **Caldicott requirements**, and employees' responsibilities for **confidentiality** and the safeguarding of confidential information held both manually (non-computerised structured filing system) and electronically. Acceptable use of the Council's IT infrastructure systems is detailed within the Acceptable Use Policy and should be read in conjunction with the policy.

The Council holds and manages a great deal of personal and confidential information relating to citizens, service users and carers, the public and employees. Personal data is data that relates to an identified or identifiable individual and is:

- Processed electronically,
- Kept in a filing system,
- Part of an accessible record, for example an education record.

Data protection laws exist to strike a balance between the rights of individuals to privacy and the ability of organisations, like the Council, to use data in order to meet its legal obligations and for legitimate business purposes.

Data protection legislation is concerned with 'personal data' which means any information relating to an 'identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an 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'.

Information relating to a deceased person does not constitute personal data and therefore is not subject to the GDPR or DPA.

The GDPR is divided into "Recitals" and "Articles" and works in two ways, (1) giving individuals certain rights whilst (2) requiring those who record and use personal information certain responsibilities. The Regulation contains the following 6 *principles* which are binding for all organisations processing data:

Article 5 Principles relating to processing of personal data

Personal data shall be:

(a) Processed lawfully, fairly and in a transparent manner in relation to the data subject ('lawfulness, fairness and transparency');

(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, in accordance with Article 89(1), not be incompatible with the initial purposes ('purpose limitation');

(c) Adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed ('data minimisation');

(d) Accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data is accurate, and that any inaccuracies are erased or rectified without delay.

(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 in accordance with Article 89(1) subject to implementation of the appropriate technical and organisational measures required by this Regulation in order to safeguard the rights and freedoms of the data subject ('storage limitation');

(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').
(g)

ALL STAFF HAVE A LEGAL DUTY TO PROTECT THE PRIVACY OF INFORMATION ABOUT INDIVIDUALS

To ensure its compliance with the GDPR and the DPA, the Council:

- ✓ Has a legal basis for acquiring and/or using any personal data.
- ✓ Has a clear retention policy for handling personal data.
- ✓ Has entrusted Departmental/Service Information Asset Owners (IAOs) to ensure that information management processes are effective, that personal data is being processed in accordance with policy and that personal data is not held for longer than is necessary.
- ✓ Ensures that all staff are aware of the information retention policy and follow it.
- ✓ Has an established process for responding to subject access requests
- ✓ Has an established process for identifying, assessing and reporting any personal data breach that is likely to result in a risk to the rights and freedom of an individual, informing the ICO and, if the risk is deemed to be high, also

inform the individual concerned. *(The GDPR introduced a duty on all organisations to report certain types of personal data breach to the relevant supervisory authority within 72 hours of becoming aware of the breach, where feasible).*

- ✓ Has appointed a Data Protection Officer who will help embed, communicate and monitor the organisation's data protection policy.

3 Scope, Requirements of Legislation & Definitions

Scope

The General Data Protection Regulation (GDPR) and the Data Protection Act 2018 (DPA) apply to all personally identifiable information held in manual files, computer databases, videos and media about living individuals, such as personal records, personnel and payroll records, other manual files, microfiche/film, etc. Data referenced by any criteria that might identify a living individual, including but not limited to name and address, or reference number, constitutes personal data.

All personal data must be handled according to the GDPR and DPA requirements, and this policy sets out how this is delivered in the Council.

This policy covers all identifiable information created, processed and stored on living individuals, citizens, clients or staff. Throughout this document the term “client” is used to refer to an individual who is receiving a service from the Council, and this term includes those people who are also known as “service users”. Similarly, the term “professional” is used, but should be interpreted as encompassing staff and practitioners.

Definitions

The **General Data Protection Regulations (GDPR)** provide controls on the handling of personal identifiable information for all **living** individuals. Central to the Act is compliance with the principles (Article 5), designed to protect the rights of individuals about whom personal data is processed whether an electronic or a paper record.

The **Data Protection Act 2018** implements the EU's General Data Protection Regulation (GDPR), while providing for certain permitted derogations, additions and UK-specific provisions.

The **Caldicott Report 1997 and subsequent reviews** provides guidance on the use and protection of personal confidential data, and emphasises the need for controls over the availability of such information and access to it. It makes a series of recommendations which led to the requirement for organisations to appoint a **Caldicott Guardian** who is responsible for compliance with the Caldicott confidentiality principles.

The **Common Law Duty of Confidentiality** prohibits use and disclosure of information, provided in confidence unless there is a statutory requirement or court order to do so. Such information may be disclosed only for purposes that the subject

has been informed about and has consented to, provided also that there are no statutory restrictions on disclosure. This duty is not absolute but should only be overridden if the holder of the information can justify disclosure as being in the public interest, for example, to protect the vital interests of the data subject or another person, or for the prevention or detection of a serious crime.

4 Duties and Responsibilities

The Council has established a framework and structure to deliver information governance, to meet the requirements of data protection and confidentiality.

Framework:

Information Management Executive Group

The Corporate Information Management & Governance Executive Group (IMG Executive) is a group of senior Council officers chaired alternatively by the Head of Strategic Support and Senior Information Risk Owner (SIRO) that reports to the Senior Leadership Board (SLB) and the Audit & Governance Committee (A&G). It is implemented - as recommended by Government - with the role of overseeing the Information Management & Governance framework for the Council.

Information Management Tactical Group

The Corporate Information Management & Governance Tactical Group (CIMGTaG) is a sub-group of the Corporate Information Management & Governance Executive Group (CIMGEG) and provides tactical and operational support for strategic decisions made by the Executive Group.

The Corporate Information Management & Governance Tactical Group is chaired by the SIRO and reports to the IMG Executive. It has the role of implementing the Information Management & Governance framework for the Council and advising the IMG Executive on matters of Information Management & Governance covering control, compliance, and prevention of legal failure.

Structure: The Chief Executive

The Chief Executive has overall responsibility for Data Protection within Sefton Council. The implementation of, and compliance with this policy is delegated to the Senior Manager ICT and Digital (ICT Client Unit | Finance & Information Services) who is designated as Sefton Council's Senior Information Risk Owner (SIRO). The Council's Chief Legal and Democratic Officer acts as the Deputy SIRO.

Senior Information Risk Owner (SIRO)

The SIRO role is an integral part of the Council's Information Governance Framework, accountable for information asset risks, actively working with relevant experts across the organisations to determine the most effective and proportionate information control measures; The SIRO has a duty to ensure they:

- Develop a culture to secure and protect information for the benefit of the organisation and its customers
- Be Responsible for the risk and incident management governance
- Support the development of the corporate Risk Policy and risk assessment process
- Staff are aware of the need to comply with the GDPR, in particular with the rights of clients wishing to access personal information and or their care records.
- Staff are aware of requirements of the common law duty of confidentiality.
- Arrangements with third parties who process personal data on behalf of the Council are subject to a written contract which stipulates appropriate security and confidentiality of information.
- Ensuring the IMG Executive are informed of relevant issues and that associated decisions are recorded.
- Maintaining an Information Asset Register

Caldicott Guardian

The Council's Caldicott Guardian is an Adult Social Care Service Manager. The Caldicott Guardian is responsible for agreeing and reviewing protocols for governing the transfer and disclosure of personal confidential data in relation to health and social care across the Council and supporting agencies.

Data Protection Officer

The Council's Data Protection Officer has responsibility for implementing the activities necessary to achieve compliance with the GDPR throughout the Council. These include, but are not restricted to:

- Informing and advising the organisation and its employees about their obligations in order to comply with data protection legislation.
- Provide advice in the event of a data breach, including reporting to the ICO when applicable
- Assisting individual services with the production of privacy notices relevant to their processing activity.
- Monitoring compliance with the GDPR and other data protection laws, including managing internal data protection activities, advising on data protection impact assessments; information sharing agreements, training staff and conducting internal audits.
- Being the first point of contact for supervisory authorities and for individuals whose data is processed (citizens/clients/staff).
- Ensuring the Council's data protection fee is paid to the Information Commissioner's Office
- Responsibility for co-ordinating the return of the annual Data Security & Protection Toolkit (DS&PT) via the NHS Digital on-line self-assessment portal.
- Carrying out data protection and compliance checks across the Council's various departments, as required.
- Developing the process for responding to subject access requests, right to rectification, erasure, restrict processing, data portability or

right to object.
- Maintaining Records of Processing Activities (ROPA).

The Information Management and Governance (IMG) Executive

The IMG Executive is responsible for Information Governance and Assurance. This includes:

- Facilitating all the Data Protection and Caldicott functions within the Council to support the above.
- Advising the Council in relation to directives/guidance from the Information Commissioner and the Department of Health.
- Ensuring effective training is provided to all staff in information compliance requirements
- Ensuring that the Council's personnel are aware of their responsibilities and accountability for information management and confidentiality.

Information Security Lead

The Senior Manager ICT and Digital is responsible for ICT Security. This includes:

- Providing an advisory service to the Information Governance Executive.
- Monitoring and reporting on the state of Information Management & Technology (IM&T) security within the organisation.
- Ensuring that the Council's Information Security Policy is maintained, up to date and implemented throughout the organisation.
- Developing and enforcing detailed procedures to maintain information security.
- Ensuring compliance with relevant legislation.
- Ensuring that the Council's personnel are aware of their responsibilities and accountability for information security.
- Monitoring for actual or potential information security breaches related to Information Management & Technology (IM&T) security infrastructure within the organisation.
- Leading on issues regarding Cyber Security.

Information Management

Heads of Service and Service Managers are responsible for managing information within their respective Services ensuring:

- Compliance with relevant Information Management, Retention, Confidentiality and Information Security policies.
- That staff complete mandatory IG training and complete their annual online refresher training
- That data breaches and IM issues raised by staff are acted upon.
- That Information Asset Owners (IAOs) and Information Asset Administrators (IAAs) are appointed.

All Managers are responsible for ensuring that this policy is communicated and implemented within their area of responsibility. They are responsible for the quality,

security and management of personal data in use in their area. Advice or assistance regarding this policy or the General Data Protection Regulations (GDPR) is available from the Data Protection Officer (DPO).

The departmental (Service) Information Asset Owners (IAOs) are responsible for maintaining records of processing activity in their respective Service, carrying out risk assessments and providing reports to the SIRO on measures taken to mitigate or deal with information risks. The GDPR contains explicit provisions about documenting processing activities. IAOs must maintain records of processing activities, data sharing, retention schedules and may be required to make the records available to the ICO on request. The ROPA must document the following information:

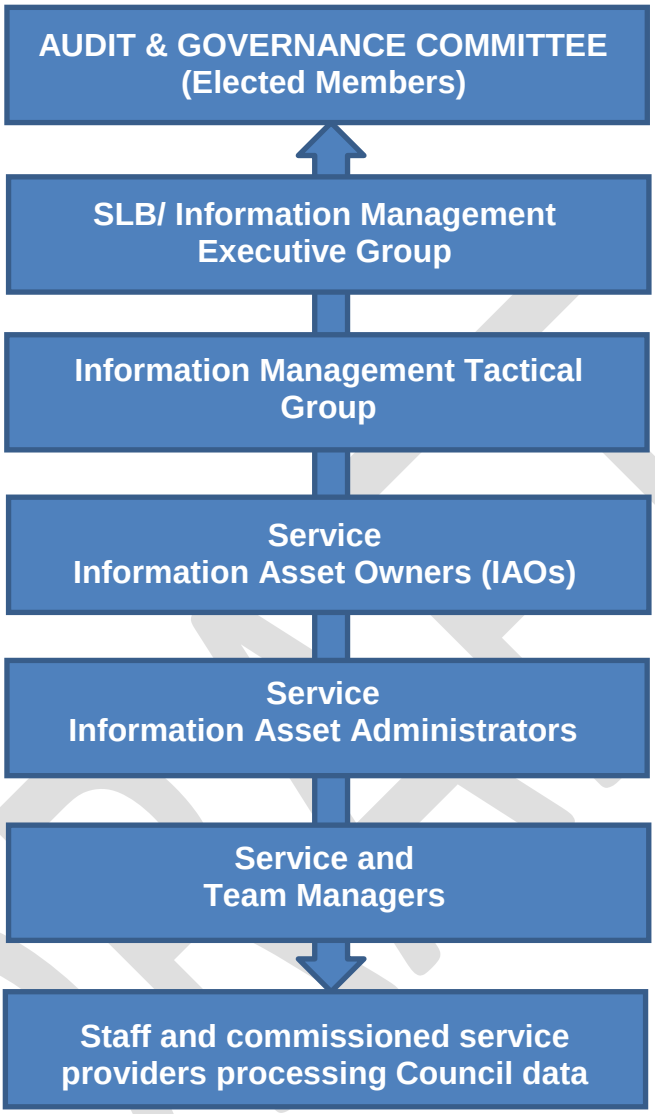
- The name and contact details of the Service (and where applicable, of other controllers or processors represented).
- The purposes of processing.
- A description of the categories of individuals and categories of personal data.
- The categories of recipients of personal data.
- Details of any transfers to third countries including documenting the transfer mechanism safeguards in place.
- Retention schedules.
- A description of the technical and organisational security measures.
- Information required for privacy notices, such as:
    - the lawful basis for the processing
    - the legitimate interests for the processing
    - individuals' rights
    - the existence of automated decision-making, including profiling
    - the source of the personal data
- Records of consent
- The location of personal data
- Data Protection Impact Assessment reports
  Records of personal data breaches
- Information required for processing special category data or criminal conviction and offence data under the Data Protection Act, covering:
    - the condition for processing in the Data Protection Act
    - the lawful basis for the processing in the GDPR
    - their retention and erasure policy document

Some of the information required for the ROPA will be relevant to the whole Council and will therefore be available from the Data Protection Officer.

All staff have a responsibility to ensure that their activities comply with the data protection principles. All staff have responsibility for the type of personal data they collect and how they use it. Staff should not disclose personal data outside the organisation's procedures, or use personal data held on others for their own purposes.

Information Governance Structure

The Information Governance structure for the Council is summarised below.



Requests for personal data are dealt with by either the relevant Information Asset Owner/Administrator (IAO/A), or the designated officer within the respective Service area. Requests for access to closed Adult Social Care files or Children's Social Care files are handled by dedicated Access to Files Officers. Advice on disclosure may be sought from the Data Protection Officer.

All data protection and information related incidents should be reported and properly investigated in accordance with the Council's incident management procedures available on the intranet.

http://intranet.smbc.loc/our-council/data-protection-information-handling/data-breach.aspx

All correspondence with the Information Commissioner on data protection related matters will be dealt with by the Data Protection Officer.

5 Data Protection

This policy sets out the framework to ensure that the Council complies with the law. This policy will be reviewed annually by the Information Management Executive group and when appropriate to consider changes to legislation that may occur, and/or guidance from the Government and/or the Information Commissioner.

The Principles::

The Council has procedures in place to ensure the principles in the GDPR and DPA are met.

5.1.a Personal data shall be:

> a) **Processed lawfully, fairly and in a transparent manner** in relation to the data subject ('lawfulness, fairness and transparency');

Compliance is achieved by:

- Ensuring the Council's Privacy Notice (available on the website) is kept up to date and complies with the law. The Council has a Data Protection Officer (DPO), whose contact details are available to the public. The DPO will also assist individual services with the production of privacy notices relevant to their processing activity.
- Complying with the common law duty of confidentiality; that any personal information given or received in confidence for one purpose may not be used for a different purpose or passed on to anyone else without the consent of the individual.
- Ensuring that the legal basis for the processing of information is identified, via the completion of the Records of Processing Activities.
- Conducting Data Protection Impact Assessments (DPIAs) whenever we undertake a project which involves processing of personal data
- Ensuring that relevant Information Sharing Agreements are implemented where processing of data is undertaken by a third party or partner agency.

Under data protection legislation, data subjects have certain rights, which must be upheld:

- The Right to be Informed – via Privacy Notcies
- Right of Access to information – (Subject Access Requests).
- Right to Rectification - to have inaccuracies corrected.
- Right to Erasure - to have information erased (right to be forgotten).
- Right to Object to processing (e.g. direct marketing).
- Right to Prevent automated decision-making and profiling.
- Right to Data portability – have information provided in electronic format and not hinder the data subject's transmission of personal data to a new data controller.

Informing Data subjects

Data subjects must be made aware of how their data will be used by Sefton Council directly. This is typically achieved via a Privacy Notice. When information is collected from data subjects whether verbally or collected on a particular form, a clear explanation should be provided about how the data will be used. Data subjects can also be informed using data subject information leaflets, either provided directly or made available in data subject areas. Where appropriate, information posters in data subject waiting areas, and statements in data subject handbooks/on survey forms can also be used.

Sefton Council is obliged to make the public aware of how it uses personal data, and to ensure that they are properly informed with whom their data is shared. The Council Generic Privacy Notice is available on the Sefton Council web site

https://www.sefton.gov.uk/your-council/plans-policies/privacy-notice.aspx.

Further guidance about privacy notices is available on the Council intranet http://intranet.smbc.loc/our-council/data-handling-foi/gdpr-(general-data-protection-regulation).aspx or by contacting the Council's DPO.

Staff

All staff, including temporary employees should be told the purposes for which their data will be used, and to whom it may be disclosed. This may occur during induction or by their manager. Workers have a right to access information that an employer may hold on them. This could include information regarding any grievances or disciplinary action, or information obtained through monitoring processes. If a worker wants to see their personal data, they should speak to their manager. Most requests for personal data can be provided quickly and easily.

Disclosure of Information without consent

Information about identifiable individuals (including data subjects and staff) should only be disclosed on a need to know basis.

Disclosures of information may occur because of a legal requirement e.g. with a Court Order. Specific legislation covers some disclosure of staff information (e.g. for tax and pension purposes) and data subjects (e.g. notifiable diseases).

The validity of all requests for disclosure of personal data without consent must be checked. The identity of those requesting data, and their legal right to request information must be validated. The reasons for disclosures made without consent must be documented.

Police officers or others requesting information for the purposes of a criminal investigation, including for benefit, tax or immigration offences, should be asked to put their request in writing, either by using a standard data protection request form, or by letter / email. This requirement can be set aside where the request is made in an emergency (i.e. a person is in immediate and imminent risk of serious harm).

The request should include:

- What information is needed
- Why it is needed
- How the investigation will be prejudiced without it

Subject Access

Individuals have a right to request any personal data held by Sefton Council in whatever form. Sefton Council has a procedure to deal with the right of access to information https://www.sefton.gov.uk/social-care/access-to-personal-files.aspx All subject access requests must be overseen by the IAO/A of a relevant service area of the Council and advice may be sought from the Council's DPO. All requests should be administered via the 'iCasework' Manage My Request system.

Exercised Rights to Rectification, Erasure or Object to Processing

Individuals have several rights, including subject access, preventing processing likely to cause harm or distress, preventing direct marketing, the right to seek compensation for breaches of data protection legislation which have caused damage or distress, and a right to take action to rectify, block, erase or destroy inaccurate data.

Where consumers exercise a right under the legislation such as the right to rectification, erasure, restrict processing, data portability or right to object these will be managed though the 'iCaseWork' case management solution.

Cases will be logged through the Council's website and the Contact Centre. Cases will then be allocated to service areas, with specific tasks or responses within a case further allocated to teams or individuals as appropriate.

Acknowledgements, responses and other correspondence will be automatically generated at the appropriate step of each process. Target timescales will be pre-defined to meet regulatory requirements, with the system enabling progress to be monitored for teams or individuals using management reports and dashboards.

Direct Marketing

Sefton Council is obliged to cease sending correspondence for the purposes of direct marketing if an individual indicates that they no longer wish to receive it. Direct marketing is defined in the Data Protection Act 2018 as:

'*the communication (by whatever means) of advertising or marketing material which is directed to particular individuals*'

All advertising or promotional material is covered, including promoting the aims or ideals of not-for-profit organisations – for example, it covers a charity or political party campaigning for support or funds.

Complaints about handling of personal data

Any complaints regarding how an individual's personal data has been handled, must be shared with the DPO. Any complaints which the Information Commissioner's Office receives directly, will be sent to the DPO to deal with.

5.1.b Personal data shall be:

> (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, in accordance with Article 89(1), not be considered to be incompatible with the initial purposes ('purpose limitation');

This will be achieved by completion of Data Privacy Impact Assessments (DPIA), which will be adopted at the implementation or change to a business system or process for collecting, processing and sharing information, and regularly reviewed. Further information regarding DPIA can be found in section9 on this policy.

Payment of the data protection fee

Under the Data Protection (Charges and Information) Regulations 2018 the Council no longer needs to notify the Information Commissioner's Office but must pay a fee. The fees paid by data controllers funds the work of the Information Commissioner's Office. Failure to pay the fee is an offence and the Council would be fined for non-payment The Data Protection Officer is responsible for ensuring the fee is paid.

5.1.c Personal data shall be:

> (c) **Adequate, relevant and limited to what is necessary** in relation to the purposes for which they are processed ('data minimisation');

This is achieved by:

- Conducting routine audits as part of good data management practice.
- Ensuring that relevant records policies and professional guidelines, i.e. information retention are adhered to.

Managers should ensure that any data collected from individuals is complete, and that the level of data retained on Sefton Council in its information systems is required for current, existing purposes, and sufficient to support appropriate and effective decisions.

Information Assets Owners (IAOs) will be responsible for conducting routine 'spot checks' and audits of information management practice and processing activities. The Council's Data Protection Officer will request evidence of the same and conduct independent audits of data processing activities across the Council.

5.1.d Personal data shall be:

> (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');

This is achieved by:

- All staff recording information accurately and taking reasonable steps to check the accuracy of information they receive and record from data subjects or anyone else.

Managers must seek to ensure that personal data held on any media is accurate and up to date by carrying out their own quality assurance and participating as required in quality assurance processes. The accuracy of personal data can be achieved by implementing validation routines, some of which will be system specific and details must be provided of these validation processes to the system/information users.

5.1.e Personal data shall be:

> (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 in accordance with Article 89(1) subject to implementation of the appropriate technical and organisational measures required by this Regulation in order to safeguard the rights and freedoms of the data subject ('storage limitation');

This is achieved by:

- Data users regularly checking all systems to destroy out-of-date information and correcting inaccurate information.
- Compliance with the Council's information retention schedule.

Personal data must not be retained indefinitely, and managers must ensure that they and their staff are aware of, and compliant with Sefton Council's Records Retention Policy. Further details of how this affects Sefton Council, and actions required to comply with it, are detailed in the Record Keeping Policy. http://intranet.smbc.loc/our-council/data-handling-foi/records-management.aspx

5.1.f Personal data shall be:

> (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').

This is achieved by:

- Compliance with the Council's Information Security Policy, Acceptable Use Policy and associated procedures
- Completion of a Data Privacy Impact Assessment where applicable.

Security

All information relating to identifiable individuals must be kept secure always. Managers must take steps to ensure that office environments and working practices take account of the security necessary to prevent the loss, theft, damage or unauthorised access to data subject and other information. Information Asset Owners are responsible for ensuring that all systems storing personal data, or other assets or repositories of information are appropriately risk-assessed and protected from identifiable threats.

Security measures include (but are not limited to) the following:

- All software and data should be removed from redundant hardware and media storage before being disposed of.
- Personal information must not be held on removable media unless encrypted (e.g. memory sticks, laptops, discs etc.).
- Personal data must not be stored on computer hard drives unless encrypted. Access to both computer and paper records should be restricted only to those who need direct access to the data contained within them.
- Access controls like passwords, smart cards and other similar measures must not be shared.
- Passwords and other security information must not be written down.
- Offices where paper records are stored must be secure, and adequate measures must be in place to prevent the loss or theft of records – measures include controlling access to premises, checking the identity of individuals visiting premises, and locking away paper records when not in use. Managers are responsible for assessing the risk of premises where their staff work, and taking remedial action.
- All confidential waste paper must be shredded.
- All actual and potential incidents must be reported via IAO/A or Data Protection Officer.

As we have moved towards a greater emphasis on Agile Working, the Council has embraced the concept of a paperless office (or "paper-free" office); a work environment in which the use of paper is eliminated or greatly reduced, by converting documents and other paper records into digital form, reducing the physical space taken by bulky filing cabinets and storage systems.

Going paperless is an exciting process that can revolutionise the way individuals and the organisation could work daily, but it is recognised that the transition to paperless is a significant task across the whole Council. To assist the process the Council has established three new frameworks for **(1)** the secure destruction of confidential waste, **(2)** off-site document storage and **(3)** Scan on demand document image processing. These framework agreements can be accessed on the corporate framework agreements page.

Guidance on the process for reviewing, categorising and processing existing paper records can be found on the Council's Intranet http://intranet.smbc.loc/intranet-features/news/document-management.aspx

However, were there is an identified need to retain or work with paper records then these records must be kept in locked filing cabinets or locked drawers. This includes notebooks, copies of correspondence and any other sources of information that contains personal identifiable information.

Information Security

The ICT Client Services are responsible for ensuring that systems under the control of Sefton Council and the 'users' of those systems comply with current data protection legislation and Principles. This includes responsibility for ensuring that procedures and technical measures are in place to achieve a high level of data integrity.

The ICT Client will ensure that:

- 'Users' are set up on IT system will appropriate access control relative to their position and duties; ensuring that relevant information is accessible on 'a need to know basis'.
- Audit information is readily available on request to support any investigation into inappropriate access to an IT system and associated data/records.
- Advice is sought from the Data Protection Officer whenever appropriate and that data protection implications are considered at the earliest stage whenever systems are procured or altered.
- Reporting and disclosures of data/information from ICT system is limited to those performing a business intelligence and performance management function.
- Unusual requests for disclosure are scrutinised and referred to the IAO and Data Protection Officer when necessary.
- IT support staff are aware of their responsibilities regarding information security, data protection and client confidentiality.

Information Asset Owners have been advised of their responsibilities to carry out a risk assessment on the information asset (system) for which they are responsible, in accordance with the Sefton Council's Information Risk Policy and Risk Management Policy.

Data Back-ups and Recovery

IT Services are responsible for ensuring there is a procedure which outlines the

media, frequency, retention period and control measures for back-ups of the data and system configuration within their control.

Information in Transit

Hardcopy data subject or other sensitive personal data must only be sent by recorded delivery and must be properly addressed to a named individual. Reliable transport couriers must be used always. Packaging should be sufficient to protect the contents from any physical damage during transit,

Contracts between Sefton Council and third parties must include an appropriate confidentiality clause which should be disseminated to the third parties' employees.

Data Processors

Where Sefton Council uses a contractor to process personal data on its behalf, the contractor must sign a contract or 'data processing agreement' which ensures that they are taking adequate steps to comply with GDPR on Sefton Council's behalf.

Further information regarding the Council's Information and ICT Security is available on the Council intranet http://intranet.smbc.loc/our-council/data-handling-foi/policies.aspx

6 Caldicott Principles for handling personal confidential data.

The Caldicott Principles were developed in 1997 following a review of how patient information was handled across the NHS. The Review Panel (chaired by Dame Fiona Caldicott) set out six Principles that organisations should follow to ensure that information that can identify a patient is protected and only used when it is appropriate to do so. Since then, when deciding whether they needed to use information that would identify an individual, an organisation should use the Principles as a test. The Principles were extended to Adult Social Care records in 2000. These principles apply equally as a guide to other Services across the Council when processing personal confidential data. The Caldicott Principles revised 2013 are:

1 - Justify the purpose(s) for using confidential information

Every proposed use or transfer of personal confidential data within or from an organisation should be clearly defined, scrutinised and documented, with continuing uses regularly reviewed, by an appropriate guardian.

2 - Don't use personal confidential data unless it is absolutely necessary

Personal confidential data items should not be included unless it is essential for the specified purpose(s) of that flow. The need for patients to be identified should be considered at each stage of satisfying the purpose(s).

3 - Use the minimum necessary personal confidential data

Where use of personal confidential data is essential, the inclusion of each individual item of data should be considered and justified so that the minimum amount of personal confidential data is transferred or accessible as is necessary for a given function to be carried out.

4 - Access to personal confidential data should be on a strict need-to-know basis

Only those individuals who need access to personal confidential data should have access to it, and they should only have access to the data items that they need to see. This may mean introducing access controls or splitting data flows where one data flow is used for several purposes.

5 - Everyone with access to personal confidential data should be aware of their responsibilities

Action should be taken to ensure that those handling personal confidential data - both clinical and non-clinical staff - are made fully aware of their responsibilities and obligations to respect patient confidentiality.

6 - Comply with the law

Every use of personal confidential data must be lawful. Someone in each organisation handling personal confidential data should be responsible for ensuring that the organisation complies with legal requirements.

In April 2013, Dame Fiona Caldicott reported on her second review of information governance, her report "Information: To Share or Not to Share? The Information Governance Review", informally known as the Caldicott2 Review, introduced a new 7th Caldicott Principle.

7 - The duty to share information can be as important as the duty to protect patient confidentiality

Health and social care professionals should have the confidence to share information in the best interests of their patients within the framework set out by these principles. They should be supported by the policies of their employers, regulators and professional bodies.

The Health and Social Care (Safety and Quality) Act 2015 includes a legal duty that requires local Health and Adult Social Care bodies to share information where this will facilitate improved care for an individual.

7 Confidentiality

The Council holds personal data about its staff, clients, members etc. GDPR and the Data Protection Act 2018 place a responsibility on the Council to ensure the confidentiality of its clients, insofar that no information given to the Council will be shared with any other organisation or individual without the user's express permission or where another lawful basis exists.

For this policy, confidentiality relates to the transmission of personal, sensitive or identifiable information about individuals or organisations (confidential information), which comes into the possession of the Council and its employees through its work.

All personal data will be dealt with sensitively and in the strictest confidence internally and externally.

Purpose

The purpose of the Confidentiality Policy is to ensure that all staff, members, volunteers and users understand the Council's requirements in relation to the disclosure of personal data and confidential information.

Principles

- All personal data (paper-based and electronic) must be processed and stored in accordance with the GDPR and DPA and must be secured against unauthorised access, accidental disclosure, loss or destruction.

- All personal paper-based and electronic data must only be accessible to those individuals authorised to have access.

Following the publication of the Caldicott Review in March 2013, the Health & Social Care Information Centre published "A guide to confidentiality in Health and Social Care" which identified five rules for treating confidential information with respect. These same rules are applicable in practice to all areas the Council and include:

- **Rule 1:** Confidential information about service users should be treated confidentially and respectfully.

- **Rule 2:** Member of a Care Team should share confidential information when it is needed for the safe and effective care of an individual.

- **Rule 3:** Information that is shared for the benefit of the community should be anonymised.

- **Rule 4:** An individual's right to object to the sharing of confidential information about them should be respected.

- **Rule 5:** Organisations should put policies, procedures and systems in place to ensure the confidentiality rules are followed.

Client Confidentiality

Information that the Council collects in confidence from clients attracts a **common law duty of confidence** until it has been effectively anonymised. This legal duty prohibits information use and disclosure without consent, effectively providing individuals with a degree of control over who sees information that they provide in confidence. This duty can only be overridden if there is a statutory requirement, a court order, or if there is a robust public interest justification.

At first contact with the service for a matter, all clients should be asked if they consent to their information being recorded and shared with other key partner agencies in the interest of supporting their need and progressing a satisfactory resolution. This information must be recorded in the relevant client record.

In the event of a client being unable to give permission, the Mental Capacity Act 2005 must be followed.

In all cases, the wishes expressed must be appropriately documented in the client's record.

Staff Confidentiality

All staff are required to keep confidential any information regarding clients and other staff, only informing those that have a need to know Telephone conversations and electronic communications should be conducted in a confidential manner.

Confidential information must not be disclosed to unauthorised parties without prior discussion and confirmation with a Senior Manager in the Council. Staff must not process any personal information in contravention of the GDPR.

Staff must not access client or staff information on any system (electronic or paper) that relates to family (including spouses; children; parents etc.) or friends, even if it is within their role in the organisation.

Any breaches of these requirements will potentially be regarded as serious misconduct and as such may result in disciplinary action.

All staff have a confidentiality clause in their contract of employment.

The Council must have an approved Data Protection and Confidentiality clause in all contracts with 3rd party contractors and suppliers who process personal information on behalf of the Council in undertaking the contracted works or provision of goods and services.

Exemptions to Confidentiality

In certain circumstances, personal information may be disclosed and guidance is provided below. However, it is vital in each case that staff assess the need to disclose the information and document that the information has been released to whom and for what reason. If they are in any doubt, they should seek advice from their Team Manager, the Caldicott Guardian or the Council's Data Protection Officer.

Disclosing Information against the Subject's wishes

The Council recognises that occasions may arise where individual workers feel they need to breach confidentiality. Confidential or sensitive information relating to an individual may be divulged where there is risk of danger to the individual, a volunteer or employee, or the public at large, or where it is against the law to withhold it. In these circumstances, information may be divulged to other agencies or departments e.g. Police or Social Services, on a need to know basis.

The responsibility to withhold or disclose information without a data subject's consent must be made by a Senior Manager in the respective service and cannot be delegated. Circumstances where the subject's right to confidentiality may be overridden are rare. Examples of these situations are:

- Where the subject's life may be in danger, or cases in which s/he may not be capable of forming an appropriate decision.
- Where there is danger to other people.
- Where the rights of others may supersede those of the subject, for example a risk to children or the serious misuse of substances.
- Where there is a serious threat to a professional or other staff.
- Where there is a serious threat to the community.
- In other exceptional circumstances, based on professional consideration and consultation.

Where an employee of the Council feels confidentiality should be breached the following steps will be taken:

- The worker should raise the matter immediately with their Line Manager.
- The worker must discuss with the Line Manager the issues involved in the case and explain why it is necessary to breach confidentiality
- The Line Manager is responsible for discussing with the worker what options are available in each set of circumstances.
- If the Line Manager lacks sufficient seniority for deciding whether confidentiality should be breached they must escalate to their Service Manager
- Advice should be sought from the Data Protection Officer

If in doubt, staff should seek guidance, in confidence, from the appropriate Team Manager, the Caldicott Guardian or the Council's Data Protection Officer.

The Council will support any member of staff who, after using careful consideration, professional judgement, and has sought guidance from their manager, can satisfactorily justify and has documented any decision to disclose or withhold information against a client's wishes.

National Data Opt-out

The National Data Opt-out is a service that enables the public to register to opt out of their confidential patient information being used for purposes beyond their individual

care and treatment. It was introduced for the health and social care system in England on 25 May 2018. The public can change their national data opt-out choice at any time.

Its purpose is to give the public a choice about whether their confidential patient information is shared for research and planning.

The national data opt-out applies to data for patients/clients where their care is provided in England by a publicly funded organisation or the care has been arranged by a public body such as the NHS or a Local Authority, it does not apply to data related to private patients/clients at private providers.

In summary the national data opt-out applies to:

- all NHS organisations (including private patients treated within such organisations)
- all Local Authorities providing publicly funded care
- adult social care providers where the care provided is funded or arranged by a public body
- private or charitable healthcare providers providing NHS funded treatment or arranged care

Which data disclosures do national data opt-outs apply to?

National data opt-outs apply to a disclosure when an organisation e.g. a research body confirms they have approval from the Confidentiality Advisory Group (CAG) for the disclosure of confidential patient information held by another organisation responsible for the data (the data controller) such as an NHS Trust.

The CAG approval is also known as a section 251 approval and refers to section 251 of the National Health Service Act 2006 and its current Regulations, the Health Service (Control of Patient Information) Regulations 2002. The NHS Act 2006 and the Regulations enable the common law duty of confidentiality to be temporarily lifted so that confidential patient information can be disclosed without the data controller being in breach of the common law duty of confidentiality.

In practice, this means that where we (the Council) are responsible for the information (as the data controller) we can, if we wish, disclose the information to the data applicant e.g. research body without being in breach of the common law duty of confidentiality. It is only in these cases where opt-outs apply.

National data opt-outs do not apply where:

- information being disclosed is anonymised in accordance with the Information Commissioner's Office anonymisation code of practice

- the individual has given their consent for their information to be used for a particular purpose, e.g. a specific research study

- there is an overriding public interest in the disclosure, i.e. the public interest in disclosing the data overrides the public interest in maintaining confidentiality, also referred to as the 'public interest test'

- there is a legal requirement that sets aside the common law duty of confidentiality or the information is required by a court order.

In these scenarios above, section 251 approvals would not have been sought.

Individuals are informed of this right in the Adult Social Care Privacy Notice which is available on the Council's website.

Children & Young People Consent and confidentiality

Children and young people have the same rights to and expectations of confidentiality as any other. Judgements need to be made on a case-by-case basis about circumstances when it might be appropriate to share information with parents or carers.

Safeguarding

Sharing of information between practitioners is essential to ensure that children and vulnerable adults are properly protected. Information from different sources may have to be put together to ensure that a child or vulnerable adult can be identified as being in need or at risk of harm. Where there are concerns that a child or vulnerable is, or may be at risk of significant harm, the professional must follow local safeguarding procedures.

For further information on information sharing in this context or adult safeguarding, staff should seek guidance from appropriate Managers in either Children's Services Safeguarding team http://intranet.smbc.loc/services/childrens-social-care.aspx or Adults Services safeguarding http://intranet.smbc.loc/services/adult-social-care.aspx?xpfaqs=true#faq2

Statistical Recording and Research

The Council is committed to effective statistical recording and monitoring of the use of its services to measure performance.

The legal basis for processing confidential data for health and social research is 'a task in the public interest'; '(6(1)(e) – processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller'.

All statistical records given to third parties, such as to support funding applications or monitoring reports shall be produced in anonymous form, so individuals cannot be recognised.

All project-based research within the Council must comply with the Data Protection & Caldicott Guardian Principles as set out within this Policy.

The Performance & Business Intelligence Department will log and retain as appropriate, all relevant data protection agreements and approvals for research studies, as evidence for compliance with the General Data Protection Regulation and Data Protection Act 2018.

8 Data Privacy Impact Assessment

All projects and processes that are likely to result in a high risk to individuals or use intrusive technologies must be subject to a Data Privacy Impact Assessment (DPIA). DPIAs must be reviewed by the Data Protection Officer and SIRO prior to the work commencing.

Data Privacy Impact Assessments (for paper and digital data) is an analysis of how personally identifiable information is collected, used, shared, and maintained:

I. To ensure handling conforms to applicable legal, regulatory, and policy requirements regarding privacy.
II. To determine the risks and effects of collecting, maintaining and disseminating information in identifiable form in an electronic information system and (iii) to examine and evaluate protections and alternative processes for handling information to mitigate potential privacy risks.

This is a method of reviewing a data project or even a database presently operating but extending its function, where access to personal data is being changed. It seeks to identify privacy risks for individuals (citizens and staff) and compliance risks for the Council.

Further information on conducting DPIAs can be seen on the ICO website, at the link below:

https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/accountability-and-governance/data-protection-impact-assessments/

Guidance on undertaking a Privacy Impact Assessment for new or existing systems can be found on the Council's Intranet

http://intranet.smbc.loc/our-council/data-protection-information-handling/guidance.aspx

9 Staff Awareness

Training

The Council will ensure that training courses and regular staff briefings are delivered to support the implementation and adoption of this policy. The training will ensure general awareness of the Data Protection and Caldicott principles with more specific training for identified roles – e.g. Social Workers, IAOs, Caldicott Guardian, Senior Information Risk Owner and Data Protection Officer.

Sefton Council has an established a mandatory training programme which includes maintaining awareness of data protection, confidentiality and security issues for all staff. This is carried out by regular training sessions covering the following subjects:

- Personal responsibilities
- Confidentiality of personal information
- Relevant Sefton Council Policies and Procedures
- Compliance with data protection principles
- Individual rights
- General good practice guidelines covering security and confidentiality
- Records management
- Process for managing potential data breaches

All staff will complete the required Information Governance on-line learning and reassessment modules:

- New staff must complete training within the first week of work
- Refresher training is undertaken annually
- Staff who commit a data breach will be instructed to attend the next available classroom-based training session

A register will be maintained of all staff attendance at training sessions.

Induction

All new starters processing personally identifying data will receive local and organisational induction on Information Governance which will include data protection, confidentiality and records management.

Contracts of Employment

Staff contracts of employment are produced and monitored by Sefton Council's Human Resources department. All contracts of employment include will a data protection and general confidentiality clause. Agency and contract staff will be subject to the same data protection and general confidentiality clause.

Disciplinary issues

All personal data recorded in any format must be handled securely and appropriately, and staff must not disclose information for any purpose outside their normal work role. Any deliberate or reckless disclosure of information by a member of staff will be considered as a breach of this Council Policy which could result in a member of staff facing disciplinary action. Managers must therefore ensure that all staff familiarise themselves with the content of this policy. Employees should be aware that it is a criminal offence to deliberately or recklessly disclose personal data without the authority of Sefton Council.

10 Monitoring Compliance

Legislative framework

The Council will monitor this policy to ensure it meets statutory and legal requirements including, but not restricted to the General Data Protection Regulation and Data Protection Act.

Data Protection legislation compliance

Compliance with the GDPR is mandatory and the Council will ensure that it keeps an up to date register of all purposes for processing personal data and makes the required notification with the Information Commissioner's Office.

Data Security and Protection Toolkit

The Council is required to complete an annual review of Information Governance compliance by completing the on-line NHS Digital Data Security and Protection Toolkit.

Reporting of data breaches

Any data breach must be reported to your Line Manager and the Council's Data Protection Officer immediately after an employee becomes aware of the incident. If it meets the threshold for reporting to the ICO, the DPO must report the breach within 72 hours of becoming aware of it. This includes completing a preliminary investigation and completing the ICO's report form Further information is available on the Council intranet http://intranet.smbc.loc/our-council/data-handling-foi/data- breach.aspx

Ensuring the effectiveness of the Policy

All staff will be alerted to and able to access the Data Protection and confidentiality policy on the Council's Intranet. Existing and new workers will be introduced to the policy via induction and training. The policy will be reviewed annually and amendments will be proposed and agreed by the Information Management Executive Group. If revised, all staff will be alerted to the new version which will always be held on the Council's intranet.

Non-adherence

Breaches of this policy will be dealt with under the Grievance and/or Disciplinary procedures as appropriate.

11 Appendix 1 - GDPR data processing - legal basis

Personal data – any information relating to an identifiable person who can be directly or indirectly identified – name; identification number, location data or online Identifier:

- The GDPR does not apply to anonymised data whereas personal data that has been pseudonymised is personal data for the purposes of GDPR. Pseudonymisation is defined as:

'*the processing of 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'*

Lawfulness of processing personal data - Article 6

6; 1 (a)	The data subject has given consent to the processing of his or her personal data for one of more specific purposes.
6; 1 (b)	Processing is necessary for the performance of a contract to which the data subject is party or to take steps at the request of the data subject prior to entering a contract
6; 1 (c)	Processing is necessary for compliance with a legal obligation to which the data controller is subject
6; 1 (d)	Processing is necessary to protect the vital interests of the data subject or of another natural person
6; 1 (e)	Processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller
6; 1 (f)	Processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child

Sensitive data – "special categories of personal data"

Processing of special categories of personal data - Article 9

1. Racial or ethnic origin; political opinions; religious or philosophical beliefs; trade union membership; processing of genetic data; biometric data (for the purpose of uniquely identifying a natural person); data concerning health; data concerning a natural person's sex life or sexual orientation – SHALL BE PROHIBITED ***[see below]

2. Paragraph 1 shall NOT APPLY if one of the following applies:

2a	**The data subject has given EXPLICIT consent to the processing of those personal data for one or more specified purposes**, except where Union or Member State law provide that the prohibition referred to in paragraph 1 may not be lifted by the data subject**.**
2b	Processing is necessary for the purposes of carrying out the obligations and exercising specific rights of the controller or of the data subject in the field of employment and social security and social protection law, in so far as it is authorised by Union or member State law or a collective agreement pursuant to Member State law providing for appropriate safeguards for the fundamental rights and the interests of the data subject.
2c	Processing is necessary to protect the vital interests of the data subject or of another natural person where the data subject is physically or legally incapable of giving consent *[Capacity Act would apply – or if the person is at risk i.e. Mental Health Act Assessment]*
2d	Processing is carried out during its legitimate activities with appropriate safeguards by a foundation, association or any other not-for-profit body with a political, philosophical, religious or trade-union aim and on condition that the processing relates solely to the members or to former members of the body or to persons who have regular contact with it in connection with its purposes and that the personal data are not disclosed outside that body without the consent of the data subjects.
2e	Processing relates to personal data which are manifestly made public by the data Subject.
2f	Processing is necessary for the establishment, exercise or defence or legal claims or whenever courts are acting in the judicial capacity.
2g	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.

2h	**Processing is necessary for the purposes of preventive or occupational medicine, or 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** *Paragraph 3: Personal data referred to in para 1 may be processed for the purposes referred to in point (h) of para 2 when those data are processed by or under the responsibility of a professional subject to the obligation of professional secrecy under Union or Member State law or rules established by national competent bodies or by another person also subject to an obligation of secrecy under Union or Member State law or rules established by national competent bodies.*
2i	Processing is necessary for reasons of public interest around public health, such as protecting against serious cross-border threats to health or ensuring high standards of quality and safety of health care and of medicinal products or medical devices, on the basis of Union or Member State law which provides for suitable and specific measures to safeguard the rights and freedoms of the data subject, professional secrecy; or
2j	Processing is necessary for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89(1) based on 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 interests of the data subject.

12 Appendix 2 Relevant Acts of Parliament

Data Protection Act 2018 (DPA)

The DPA implements the EU's General Data Protection Regulation (GDPR), while providing for certain permitted derogations, additions and UK-specific provisions.

The data protection principles are:

1) Lawfulness, fairness and transparency
2) Specified, explicit and legitimate
3) Adequate, relevant and not excessive
4) Accurate
5) Must be kept for no longer than is necessary
6) Taking appropriate security measures

Human Rights Act 2000

This Act became law on 2 October 2000. It binds public authorities to respect and protect an individual's human rights. This will include an individual's right to privacy (under Article 8) and a service user's right to expect confidentiality of their information always.

Article 8 of the Act provides that 'everyone has the right to respect for his private and family life, his home and his correspondence'. However, this article also states 'there shall be no interference by a public authority with the exercise of this right except as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety, or the economic well-being of the country, for the prevention or disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others'.

Regulation of Investigatory Powers Act 2000

This Act combines rules relating to access to protected electronic information as well as revising the 'Interception of Communications Act 1985'. The Act aims to modernise the legal regulation of interception of communications in the light of the Human Rights laws and rapidly changing technology.

Crime and Disorder Act 1998

This Act introduces measures to reduce crime and disorder, including the introduction of local crime partnerships around local authority boundaries to formulate and implement strategies for reducing crime and disorder in that local area.

The Act allows disclosure of person identifiable information to the Police, Local Authorities, Probation Service or the Health Service but only if the purposes are defined within the Crime and Disorder Act. The Act does not impose a legal requirement to disclose/exchange person identifiable information and responsibility

for disclosure rests with the organisation holding the information. There should be a Crime and Disorder Protocol governing the disclosure/exchange and use of personal information within a local authority boundary agreed and signed by all involved agencies and organisations.

The Computer Misuse Act 1990

This Act makes it a criminal offence to access any part of a computer system, programs and/or data that a user is not entitled to access. Each organisation will issue each user an individual user id and password which will only be known by the individual they relate to and must not be divulged / misused by other staff. This is to protect the employee from the likelihood of their inadvertently contravening this Act.

Each organisation will adhere to the requirements of the Computer Misuse Act 1990 by ensuring staff are made aware of their responsibilities regarding the misuse of computers for personal gain or other fraudulent activities. Any member of staff found to have contravened this Act will be considered to have committed a disciplinary offence and be dealt with accordingly.

Where individuals have been found to have committed serious breaches of data protection legislation, the Information Commissioner's Office has prosecuted individuals under the Computer Misuse Act 1990, in order to access a wider range of penalties e.g. a custodial sentence.

The Access to Health Records 1990

This Act gives data subject's representatives right of access to their manually held health records, in respect of information recorded on or after 1 November 1991. This Act is only applicable for access to deceased person's records. All other requests for access to information by living individuals are provided under the access provisions of the Data Protection Act .2018

Access to Medical Reports Act 1988

This Act allows those who have had a medical report produced for the purposes of employment and/or insurance to obtain a copy of the content of the report prior to it being disclosed to any potential employer and/or prospective insurance company.