London Borough of Sutton (LBS)

Data Protection Policy

1 Table of Contents

2 Introduction

The London Borough of Sutton is committed to a policy of protecting the rights and privacy of individuals (including service users, staff and others) in accordance with the requirements of the Data Protection Act 2018 and the General Data Protection Regulation (EU 2016/679). The Council needs to process certain information about its staff, service users and other individuals for administrative purposes (e.g. to recruit and pay staff, to administer services, to record progress, to collect fees, and to comply with legal obligations of the Government). To comply with the law, information about individuals must be collected and used fairly, stored safely and securely and not disclosed to any third party unlawfully.

This policy applies to all staff and service users within the People Directorate and supports staff in complying with the requirements of Data Protection Legislation. Any breach of Data Protection Legislation is considered to be an offence in which the Council can be held legally responsible. Legal liability can also be extended to individuals in certain circumstances. In the event of a breach of this policy, the Council's disciplinary procedures may apply. As a matter of good practice, other agencies and individuals working with the Council, and who have access to personal information, will be expected to have read and to comply with this policy. It is expected that all teams who deal with external providers will take responsibility for ensuring that they sign a contract agreeing to abide by this policy.

In the People Directorate the Information Governance Officer is are responsible for answering detailed queries about the use of personal information and documenting guidelines to staff about the appropriate use of personal and confidential information. Queries regarding the use of personal information should be directed to the Information Governance Officer.

3. The Role of the Caldicott Guardian in Social Care and Public Health

The Guardian plays a key role in ensuring that NHS, Councils with Social Services Responsibilities and partner organisations satisfy the highest practical standards for handling patient identifiable information. Caldicott Guardians were introduced into social care in 2002, mandated by Local Authority Circular: LAC 2002/2.

Acting as the 'conscience' of an organisation, the Guardian actively supports work to enable information sharing where it is appropriate to share, and advises on options for lawful and ethical processing of information.

The Caldicott Guardian also has a strategic role, which involves representing and championing Information Governance requirements and issues at Board and management team level.

In the LB Sutton People Directorate, the Caldicott Guardian for Children's Social Care is the Executive Head of Children's Social Care and Safeguarding. The Caldicott Guardian for Adults Social Care is the Executive Head of Adult Social Care. The Caldicott Guardian for Public Health is the Director of Public Health.

The Caldicott Guardians are responsible for overseeing information sharing in their respective divisions and ensuring that there are appropriate working procedures for staff to follow.

NHS and Social Care Caldicott Guardians are required to be registered on the publicly available National Register of Caldicott Guardians.

4. Data Protection Act 2018

The Data Protection Act 2018 came into effect on 25th May 2018, the same day as the General Data Protection regulation 2016 came into effect, and replaces the 1998 Data Protection Act as the primary piece of data protection legislation in the UK. The Data Protection Act 2018 and the General Data Protection Regulation 2016 together form current UK Data Protection Legislation, as such they must be read side by side.

The Data Protection Act originally derives from Article 8 of the Human Rights Act 1998 (the right to a private and family life). The Data Protection Act provides private and public sector entities with clear guidelines as to how personal information is to be processed in order to protect and promote individuals' right to privacy. The Act is underpinned by six principles which the council is required to comply with;

4.1. Principle one- 'Processing must be lawful and fair';

4.1.1 Fair processing

The Council will only collect personal data where there is a documented legitimate need i.e. to aide in the delivery of services requested. An appropriate lawful basis must be identified to allow the information to be processed. If special category data or criminal offence data is to be processed, an additional processing condition must be identified. The council will consider how the processing may affect the individuals concerned and is required to justify any adverse impact on individuals.

Individuals have the right to be informed about the collection and use of their personal data. This is a key transparency requirement under the GDPR. This is achieved through the use of a privacy notice. Privacy Notices supply individuals with the information required for them to provide informed consent and also provide the opportunity to 'opt-out' of processing. Privacy Notices must be provided **prior to the commencement of any data processing activity**, unless the processing is needed to fulfil a mandatory legal requirement i.e. provide emergency care or to assist the police in an investigation. Privacy Notices are a key transparency requirement under the GDPR.

The GDPR introduces requires that Information is processed 'transparently'. Transparency is closely linked to fairness. Transparent information processing is about being clear, open and honest with people from the start about who you are, and how and why you use their personal data.

Principle one also requires the Council to consider the fairness of sharing personal data with any third parties. The Council is committed to only transferring personal data to third parties where there is a legitimate need and it is the minimum necessary to complete the activity, in line with the Caldicott principles (see appendix 1). In the event that the Council decides to share data with a third party, explicit consent will always be sought from individuals involved unless it is in fulfilment of a legal requirement i.e. in an emergency situation to preserve an individual's life, or in the substantial public interest. This is in keeping with the requirements of the Common Law Duty of Confidentiality.

4.2 Principle two – 'Purposes of processing must be specified, explicit and legitimate';

4.2.1 Specified purposes

People Directorate staff will only process personal data for the purposes specified within the Privacy Policy. Where there is a need to process information for additional purposes which differ from those specified within the Privacy Notice, the change must be brought to the individual's attention well in advance of the change taking effect. The notification must be direct and explicit, in order to provide the individual with an opportunity to object. Where the need to process data has derived from a new project, a Data Protection Impact Assessment will need to be completed to ensure all privacy concerns have been considered from the outset.

4.2.2 Notification with the ICO; Data Protection Register

The Council is required to notify the Information Commissioners Office (ICO) of its intention to process personal data. From 25 May 2018, the Data Protection (Charges and Information) Regulations 2018 requires every organisation who processes personal information to pay a data protection fee to the ICO, unless they are exempt. Details of all organisations who pay the data protection fee are listed on the data protection register, which is available on the ICO Website.

4.3 Principle three- 'Personal data must be adequate, relevant and not excessive';

4.3.1 Adequate and not excessive

Information, which is not strictly necessary for the purpose for which it is obtained, should not be collected. If personal data is given or obtained which is excessive for the purpose, it should be immediately deleted or destroyed. Likewise, personal data should not be processed if it is insufficient for its intended purpose

It is the responsibility of all staff within the People Directorate to ensure that the records held continue to be relevant for the purposes they were originally collected. This requires staff to regularly review the data that they are retaining to ensure that it is still needed.

4.4 Principle four – 'Personal data must be accurate and kept up to date';

Personal data retained by the Council, must be reviewed and updated regularly. It is the responsibility of all employees to ensure that data held by the Council is accurate and kept up-to-date. Completion of appropriate assessment forms will be taken as an indication that the data contained therein is accurate. Information should be further checked for accuracy when there is communication with a service user or records are being updated.

Where a member of staff has discovered an inaccuracy in the care records, it is the responsibility of that employee to correct them immediately. Where a member of staff is unable to correct records

held, it is their responsibility to contact the relevant team to seek corrective action as soon as possible. The GDPR entitles individuals to have personal information rectified if they are inaccurate or incomplete. If a request for rectification is received it must be actioned immediately, and in any event within one month of receiving the request. Where information has been shared with external agencies; they too must be informed of the necessary rectification of their records.

Managers have a responsibility to monitor the standard of file recording of service user personal information by their staff and should do so by completion of regular file audits.

4.4.1 Special Category Data

Special consideration must be taken when processing Special Category Data and information must be protected by a higher level of security. Special Category Data is defined as the following types of information:

- Race
- Ethnic Origin
- Political opinions
- Religious or philosophical beliefs
- Trade union membership
- Genetic data or biometric data for the purpose of uniquely identifying an individual
- Data concerning health
- Data concerning a natural person's sex life or sexual orientation

Within the People Directorate, Mosaic is the central repository for storing service user sensitive personal information electronically. To ensure that information is being recorded correctly from the outset, staff are required to complete training before being granted access to systems (such as Mosaic) that are used to store and process Special Category Data . Where information is provided in paper format, the document must be scanned and saved within the Mosaic case file on the same working day of receipt.

To mitigate the risk of inaccurate data, when recording personal information, staff should ensure that they do the following:

- Recheck all data for typing errors following input
- Inform service users that if any of their contact information changes they should inform London Borough of Sutton as soon as possible.
- Inform the Business Support team if they spot any errors or duplications of a service user's information including any factual errors in the care records.
- Information, particularly contact details, including address, should be checked for accuracy when there is communication with a service user, at the point of annual review or when records are being updated

When entering information, staff should be aware that sensitive personal information may need to be shared with other professional's e.g. multidisciplinary teams or service providers in order to provide the right care/support for individual service users. As such it is imperative that individual case files are kept accurate and up to date.

4.5 Principle five- 'Personal data must be kept for no longer than is necessary';

The Council is required to ensure that the data it collects is retained in line with Legal and Regulatory requirements. A documented data retention schedule has been developed and details the Council's data retention obligations. It is available to view on the Intranet. In respect of Health and Social Care, all files (whether in hard or paper copy) must be retained, stored and destroyed in accordance with the Records Management Code of Practise for Health and Social Care 2016.

Information Asset Owners are responsible for managing information assets and regularly review their asset register for accuracy and completeness.

For adults social care records the Executive Head of Adults and Safeguarding is the Information Asset Owner (IAO) and the Caldicott Guardian.

For children's social care records, the Executive Head of Children's Services and Safeguarding is the Information Asset Owner (IAO) and the Caldicott Guardian.

For the Public Health team, the Director of Public Health is the Information Asset Owner (IAO) and the Caldicott Guardian.

4.6 Principle six- 'Personal data must be processed in a secure manner';

A key principle of the both the Data Protection Act and GDPR is that organisations process personal data securely by means of appropriate technical and organisational measures' – this is the 'security principle'.

All staff are responsible for ensuring and maintaining the security of all personal data processed by the Council. Care must be taken at all times to ensure that staff have access to only the minimum amount of data required to complete their activity. Completion of a Data Protection Impact Assessment ensures that the correct security controls have been considered and applied from the outset of processing.

It is the responsibility of all staff to ensure that personal data is not disclosed to any unauthorised third parties (in any format). Contracts between the Council and third parties include appropriate data handling and confidentiality clauses which should be disseminated to the third parties employees. Contracts of employment and Information Governance policies provide a robust framework for the appropriate management of information.

Physical and technical measures include the availability of secure email solutions such as Ironport and GCSX for staff to use. Where appropriate staff should use measures such as pseudonymisation and encryption, see section 4.14 for further details.

4.6.1 Clear Desk Requirement

In exceptional cases it may be necessary for staff to maintain hard copies of information for a short period of time. Hard copies of sensitive personal information must be removed from desks and working areas at the end of each day. They must also be removed when staff are absent from these areas for any length of time during the working day.

4.6.2 Direct marketing

Direct marketing is defined in section 122(5) of the Data Protection Act 2018 as: "the communication (by whatever means) of advertising or marketing material which is directed to particular individuals".

Article 21 of the GDPR entitles individuals to object to the processing of their personal data in a range of specified circumstances. In cases where personal data are processed for direct marketing

purposes, the right to object is absolute. If an organisation receives an objection from an individual in respect of direct marketing, they are required to cease processing for these purposes with immediate effect and there are no exceptions.

4.6.3 Compensation

Individuals have a right to seek compensation through the courts for any breach of the Act which may cause them damage and/or distress. The Council takes all breaches of its policies, procedures and legal responsibilities very seriously, see the Council's corporate complaints procedure.

4.7 Individuals Rights

The GDPR provides the following rights for individuals:

1. The right to be informed

Individuals have the right to be informed about the collection and use of their personal data. This is a key transparency requirement under the GDPR. This is achieved through the use of a privacy notice. You must provide privacy information to individuals at the time you collect their personal data from them.

2. The right of access

Individuals have the right to access their personal data. This is commonly referred to as a Subject Access Request. Individuals can make a subject access request verbally or in writing. Organisations have one month to respond to a Subject Access Request. In most circumstances these requests are free of charge. Further detailed information is available on the intranet; https://intranet.sutton.gov.uk/task/information-governance-and-gdpr/subject-access-request-procedure/

3. The right to rectification

The GDPR entitles individuals to have personal information rectified if they are inaccurate or incomplete. If a request for rectification is received it must be actioned immediately, and in any event within one month of receiving the request. Where information has been shared with external agencies; they too must be informed of the necessary rectification of their records.

4. The right to erasure

The GDPR introduces a right for individuals to have personal data erased. The right to erasure is also known as 'the right to be forgotten'. Individuals can make a request for erasure verbally or in writing. Organisations have one month to respond to a request. The right is not absolute and only applies in certain circumstances. If a request does not specifically say that it is a right to erasure

request, it is nevertheless valid and should be treated as such if it is clear that the individual is asking for their own personal data to be deleted. If you receive a request directly please forward your request on to the Data Protection Officer DPO@sutton.gov.uk who will be able to log and manage the request in accordance with the council's statutory obligations.

5. The right to restrict processing

Article 18 of the GDPR gives individuals the right to restrict the processing of their personal data in certain circumstances. This means that an individual can limit the way that an organisation uses their data. This is an alternative to requesting the erasure of their data. Individuals have the right to restrict the processing of their personal data where they have a particular reason for wanting the restriction. This may be because they have issues with the content of the information you hold or how you have processed their data. In most cases you will not be required to restrict an individual's personal data indefinitely, but will need to have the restriction in place for a certain period of time. If you receive a request to restrict processing, please contact the Information Governance Officer Tanya.campbell@sutton.gov.uk.

6. The right to data portability

The right to data portability gives individuals the right to receive personal data they have provided to the council in a structured, commonly used and machine readable format. It also gives them the right to request that the council transmits this data directly to another organisation.

The right to data portability only applies when your lawful basis for processing the information is consent **or** for the performance of a contract; **and** you are carrying out the processing by automated means (information held on paper files is excluded). If you receive a request from an individual to have electronic information transferred to another organisation please contact the LB Sutton Information Governance Officer Tanya.campbell@sutton.gov.uk.

7. The right to object

The GDPR provides individuals with the right to object to the processing of their personal data in certain circumstances. Individuals have an absolute right to stop their data being used for direct marketing. In other cases where the right to object applies organisations may be able to continue processing if they are able to demonstrate that they have a compelling reason for doing so. The council must inform individuals about their right to object.

An individual can make an objection verbally or in writing. Organisations have one calendar month to respond to an objection.

8. Rights in relation to automated decision making and profiling.

The GDPR restricts organisations from making solely automated decisions, including those based on profiling, that have a legal or similarly significant effect on individuals. For something to be solely automated there must be no human involvement in the decision-making process.

The restriction only covers solely automated individual decision-making that produces legal or similarly significant effects. These types of effect are not defined in the GDPR, but the decision must have a serious negative impact on an individual to be caught by this provision. A legal effect is

something that adversely affects someone's legal rights. Similarly significant effects are more difficult to define but would include, for example, automatic refusal of an online credit application, and e-recruiting practices without human intervention.

Because this type of processing is considered to be high-risk the GDPR requires organisations to carry out a Data Protection Impact Assessment (DPIA) to show that they have identified and assessed what those risks are and how they will address them.

Organisations can ***only*** carry out solely automated decision-making with legal or similarly significant effects if the decision is:

- Necessary for entering into or performance of a contract between an organisation and the individual;
- Authorised by law (for example, for the purposes of fraud or tax evasion); or
- Based on the individual's explicit consent.
- When using special category personal data organisations can **only** carry out processing described above if it has the individual's explicit consent; **or**
- The processing is necessary for reasons of substantial public interest.

4.8 Data Protection by design and default

The GDPR introduces new obligations that require organisations to integrate data protection concerns into every aspect of their processing activities. This approach is 'data protection by design and by default'.

Data protection by design is an approach that ensures organisations consider privacy and data protection issues at the design phase of any system, service, product or process and then throughout the lifecycle.

As expressed by the GDPR, it requires organisations to:

- Put in place appropriate technical and organisational measures designed to implement the data protection principles; and
- Integrate safeguards into their processing in order to meet the GDPR's requirements and protect the individual rights.

Data protection must be integrated into processing activities involving personal information and business practices.

Completion of Data Protection Impact Assessments at the beginning of projects which intend to make use of Personal Information are a fundamental requirement of demonstrating a Data Protection by design approach.

Only the minimum necessary personal data must be processed, and pseudonymisation must be used where possible. Processing must be transparent, and should allow individuals to clearly monitor what is being done with their data.

Data protection by default requires organisations to ensure that they only process the data that is necessary to achieve an agreed and defined specific purpose.

Organisations must consider things like:

- Adopting a 'privacy-first' approach with any default settings of systems and applications;
- Ensuring they do not provide an illusionary choice to individuals relating to the information to be processed;
- Providing individuals with sufficient controls and options to exercise their rights.

4.9 Information Flows Register and Information Asset Register

The Council is committed to respecting its data subjects' privacy and so, maintains an 'Information Flows Register' and 'Information Asset Register' see Appendix 2. The registers detail all of the routine transfers of personal information between the council and its third parties. Maintenance of the register improves the management of established information security risks and the opportunity to pre-empt future risks. The appropriate completion and management of these registers ensure compliance with article 30 of the GDPR, which requires that Records of specific processing activities are maintained.

4.10 Data Protection Impact Assessments (DPIA'S)

A Data Protection Impact Assessment (DPIA) is a process to assess and identify privacy risks to individuals in the collection, use and disclosure of information, and to put in place appropriate solutions.

A DPIA ensures that any project or proposal involving the use of personal data complies with Data Protection Legislation.

A DPIA must be carried out before any type of processing which is "likely to result in a high risk" is carried out.

In particular, the GDPR says organisations must complete a DPIA if they plan to:

- use systematic and extensive profiling with significant effects;
- process special category or criminal offence data on a large scale; or
- systematically monitor publicly accessible places on a large scale.

The ICO also requires you to do a DPIA if you plan to:

- use new technologies;
- use profiling or special category data to decide on access to services;
- profile individuals on a large scale;
- process biometric data;
- process genetic data;
- match data or combine datasets from different sources;

- collect personal data from a source other than the individual without providing them with a privacy notice ('invisible processing');
- track individuals' location or behaviour;
- profile children or target marketing or online services at them; or
- process data that might endanger the individual's physical health or safety in the event of a security breach.

It is important to remember that DPIAs are not just a compliance exercise. An effective DPIA allows you to identify and fix problems at an early stage, bringing broader benefits for both individuals and the Council.

- Your DPIA must:
- describe the nature, scope, context and purposes of the processing;
- assess necessity, proportionality and compliance measures;
- identify and assess risks to individuals; and
- identify any additional measures to mitigate those risks.
- To assess the level of risk, you must consider both the likelihood and the severity of any impact on individuals. High risk could result from either a high probability of some harm, or a lower possibility of serious harm.
- You should consult your data protection officer and, where appropriate, individuals and relevant experts. Any processors may also need to assist you.

If you identify a high risk that you cannot mitigate, you must consult the ICO before starting the processing.

- The ICO will give written advice within eight weeks, or 14 weeks in complex cases. If appropriate, we may issue a formal warning not to process the data, or ban the processing altogether.

The DPIA template and accompanying guidance for staff is available on the intranet https://intranet.sutton.gov.uk/task/information-governance-and-gdpr/section-8/

Once completed the DPIA must be shared with the Adult Social Care Information Governance Officer and the councils Data Protection Officer.

4.11 Sharing Information to Safeguard Children

Sharing information is a fundamental part of any frontline practitioners' job when working with children and young people. The decisions about how much information to share, with whom and when, can have a profound impact on individuals' lives. It could ensure that an individual receives the right services at the right time and prevent a need from becoming more acute and difficult to meet. At the other end of the spectrum it could be the difference between life and death. Poor or non-existent information sharing is a factor repeatedly flagged up as an issue in Serious Case Reviews carried out following the death of, or serious injury to, a child.

The GDPR and Data Protection Act 2018 **do not prevent, or limit, the sharing of information** for the purposes of keeping children and young people safe. To effectively share information: • all

practitioners should be confident of the processing conditions, which allow them to store, and share, the information that they need to carry out their safeguarding role. Information which is relevant to safeguarding will often be data which is considered 'special category personal data' meaning it is sensitive and personal
Where practitioners need to share special category personal data, they should be aware that the Data Protection Act 2018 includes 'safeguarding of children and individuals at risk' as a condition that allows practitioners to share information without consent

I**nformation can be shared legally without consent, if a practitioner is unable to, cannot be reasonably expected to gain consent from the individual,** or if to gain consent could place a child at risk.

Relevant personal information can be shared lawfully if it is to keep a child or individual at risk safe from neglect or physical, emotional or mental harm, or if it is protecting their physical, mental, or emotional well-being

If at any stage you are unsure about how or when to share information, you should seek advice and ensure that the outcome of the discussion is recorded. The Caldicott Guardian for Children's Social Care is the Executive Head of Children's Social Care and Safeguarding, and is responsible for overseeing information sharing in the Children's Social Care Division.

4.12 The Seven Golden Rules for Information Sharing

1) Remember that the General Data Protection Regulation (GDPR), Data Protection Act 2018 and human rights law are not barriers to justified information sharing, but provide a framework to ensure that personal information about living individuals is shared appropriately.

2. Be open and honest with the individual (and/or their family where appropriate) from the outset about why, what, how and with whom information will, or could be shared, and seek their agreement, unless it is unsafe or inappropriate to do so.

3. Seek advice from other practitioners, or your information governance lead, if you are in any doubt about sharing the information concerned, without disclosing the identity of the individual where possible.

4. Where possible, share information with consent, and where possible, respect the wishes of those who do not consent to having their information shared. Under the GDPR and Data Protection Act 2018 you may share information without consent if, in your judgement, there is a lawful basis to do so, such as where safety may be at risk. You will need to base your judgement on the facts of the case. When you are sharing or requesting personal information from someone, be clear of the basis upon which you are doing so. Where you do not have consent, be mindful that an individual might not expect information to be shared.

5. Consider safety and well-being: base your information sharing decisions on considerations of the safety and well-being of the individual and others who may be affected by their actions.

6. Necessary, proportionate, relevant, adequate, accurate, timely and secure: ensure that the information you share is necessary for the purpose for which you are sharing it, is shared only with those individuals who need to have it, is accurate and up to-date, is shared in a timely fashion, and is shared securely (see principles).

7. Keep a record of your decision and the reasons for it – whether it is to share information or not. If you decide to share, then record what you have shared, with whom and for what purpose.

Source: - Information sharing Advice for practitioners providing safeguarding services to children, young people, parents and carers (July 2018).

Each situation should be considered on a case-by-case basis. Professionals should always seek advice from the Information Governance Officer, Data Protection Officer, and those in legal services, where clarity is required. In the first instance practitioners should speak to their manager.

However the information is shared, it should always be recorded in the individual's record.

4.13 Anonymisation

Anonymisation is the process of turning data into a form which does not identify individuals and where identification is not likely to take place. This allows for a much wider use of the information.

The Data Protection Act controls how organisations use 'personal data' that is, information which allows individuals to be identified. Under the Data Protection Act the test for determining whether information relating to a living individual is 'personal data' is based entirely on the identification or likely identification of the individual.

The ICO Anonymisation Code of Practice contains comprehensive guidance for staff regarding anonymisation and provides detailed information about the different anonymisation methods which exist.

https://ico.org.uk/media/for-organisations/documents/1061/anonymisation-code.pdf

4.14 Pseudonymisation

Pseudonymisation

Pseudonymisation is the process of de-identifying data so that a coded reference or pseudonym is attached to a record to allow the data to be associated with a particular individual without the individual being identified.

When pseudonymisation techniques are consistently applied, the same pseudonym is provided for individual Service Users across different data sets and over time. This allows the linking of data sets and other information which is not available if the Service Users Data is removed completely.

This is a relatively high risk technique because the anonymised data still exists in an individual-level form. Electoral roll data, for example, could be used to reintroduce names that have been removed to the dataset fairly easily.

To effectively pseudonymise data the following actions must be taken:

An algorithm must be applied to the agreed field within the record, i.e. the Social Care Identifier to generate a pseudonymised identification number, to be used on reports for secondary use purposes.

Each field of identifiable information must have a unique pseudonym. Pseudonyms to be used in place of NHS Numbers and other fields that are to be used by staff must be of the same length and formatted on output to ensure readability

For example, in order to replace NHS Numbers in existing report formats, then the output pseudonym should generally be of the same field length, but not of the same characters; i.e. 5L7 TWX 619Z. Letters should be used within the pseudonym for an NHS number to avoid confusion with original NHS numbers.

The secondary use output must only display the pseudonymised data items that are required.

Pseudonymisation Controls:

The Peoples Directorate currently employs Pseudonymisation Controls to the following instances:

- Pseudonymisation controls are applied to Social Care Training materials which are created based on information contained in the live system.
- Pseudonymisation controls are applied to instances of the Social Care database used for testing and development.
- The Adult Social Care Local Account performance report shows how we draw on safe haven processes within our case work system (Mosaic) and turn personal identifiable information into anonymous and pseudonymous (including key coded) information in order to report to stakeholders. This enables us to make important performance information available and promote accountability while complying with the ICO's Anonymisation Code of Practice.

4.14.1 Secondary Purpose Processing

Personal Identifiable Information must be effectively anonymised for any other purpose that does not constitute a “direct care” purpose (a secondary purpose), unless the individual service user has provided their explicit consent or another lawful basis can be applied to support the justifiable use of that Personal information.

If you are intending to use personal identifiable information for Research purposes, please be aware that most research in the health and social care areas needs to be reviewed by an NHS Research Ethics Committee or the Social Care Research Ethics Committee.

Therefore you are required to contact the organisations Information Governance Officer if you intend to carry out **any secondary purpose processing on Identifiable Service User Information.**

4.15 Deceased individuals, and access to confidential records

Personal information pertaining to deceased individuals no longer falls under the scope of the Data Protection Act 2018. Requests for information about relating to deceased individuals falls under Freedom of Information Act 2000.

https://ico.org.uk/media/for-organisations/documents/1202/information-about-the-deceased-foi-eir.pdf

Please note, case law has established that even after death, the Common Law Duty of Confidentiality still applies to personal information obtained in circumstances where it is expected that a duty of confidence applies.

Three circumstances making a disclosure of confidential information lawful in these particular circumstances are:

- The executor of the estate has explicitly consented (the executor of the estate handles all financial and legal matters, according to the provisions of the will)
- where disclosure is necessary to safeguard others, or is in the public interest
- where there is a legal duty to do so, for example a court order

If you receive a request for confidential information pertaining to a deceased individual, please contact the Information Governance Officer for advice.

5. Appendix 1

Caldicott principles

In 2000 Ministerial approval was given for the Caldicott Principles to be implemented in Social Services to enable joint working to be underpinned by good information sharing between Health and Social Services. The Caldicott Guardian for Adult Social Services in Sutton is the Executive Head of Service Adults and Safeguarding. The Caldicott Principles below represent best practice for using and sharing identifiable personal information and must be applied whenever a disclosure of personal information is considered.

1. Justify the purposes(s) of using confidential information.

2. Only use it when absolutely necessary.

3. Use the minimum that is required.

4. Access should be on a strict need to know basis.

5. Everyone must understand his or her responsibilities.

6. Understand and comply with the law.

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 Social Care Guarantee for England

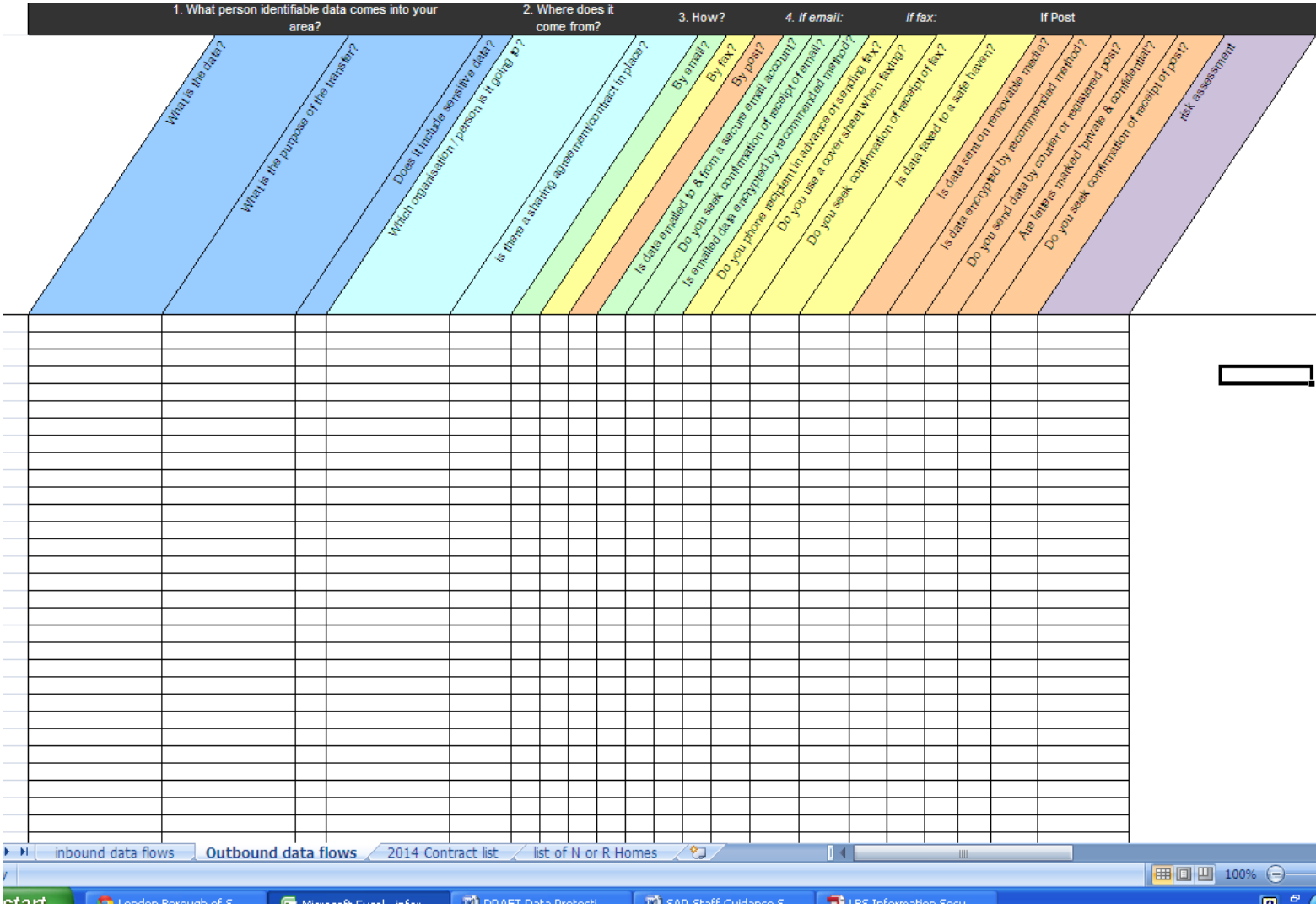
This sets out the high-level commitments for protecting and safeguarding service user information, particularly in regard to: individuals' rights of access to their own information, how information will be shared (both within and outside of the organisation) and how decisions on sharing information will be made. The following procedures must be followed by social services staff to ensure that we comply with this legislation and guidelines in our day to day work.

Documents must be appropriately marked in accordance with the corporate document marking policy.

Sharing of information must be undertaken in accordance with the corporate document handling policy.

6. Appendix 2

Information Flows Register;



7. Appendix 3

Version control

Version Control details for Information Security Policy Document			
Version No.	**Author/editor(s)**	**Approval date**	**Change summary**
v.1	Wendy Allen	15/01/15	First draft approved
v.1.1	Tanya Campbell	09/11/15	Policy revised to relate to new directorate structure 'People Directorate'
v.1.2	Tanya Campbell	09/11/15	Updated to include secondary purpose processing (3.8.1)
v.1.3	Tanya Campbell	09/11/15	Update to include clear desk requirement (3.7)
V1.4	Tanya Campbell	27/10/2016	Updated to include **Roles and Responsibilities Added:** IG Officer, Information Sharing Officer, Caldicott Guardian/ Sharing Information to Safeguard Children/ Anonymisation/ Pseudonamisation

			/Privacy Impact Assessments
V1.5	Tanya Campbell	10/10/2018	Updated to include Changes in Data Protection Legislation (DPA 2018 & GDPR) / Pseudonamisation Techniques and Requests for information pertaining to deceased service users. Inclusion of the Public Health Team