Data Protection Policy

Status

Issue 3.1

Issued by the Financial and Information Governance Team

Document Classification

Privacy & Data Protection

Document History

Issue	Change	Changed By	Authorised By
Draft 0.1	Initial Draft – No changes		
Draft 0.2	Incorporate comments from RMU	Kelly Mannix	Rachel Alexander
Draft 0.3	Incorporate comments from Distribution list	Kelly Mannix	Rachel Alexander
Draft 0.4	Incorporate comments from Distribution list	Stephen Pearson	Rachel Alexander
Draft 0.5	Incorporate comments from Senior Lawyer	Rachel Alexander	Rachel Alexander
Final 1.0			
Draft 1.1	Updated	Norman Coombe	Deborah Collins
Draft 1.2	Updated	Norman Coombe	Deborah Collins
Draft 1.3	Updated	Norman Coombe	Deborah Collins
Draft 1.4	Updated	Declan McCarthy	Deborah Collins
Draft 1.5	Updated	Norman Coombe	Deborah Collins
Draft 1.6	Updated HR concerns	Norman Coombe	Deborah Collins
Final 2.0			
Draft 2.1	Updated role of IG Manager and incorporated audit comments	Lisa Quarrell	
Draft 2.2	Incorporate comments of corporate governance panel and business manager, children's and adults services	Jo Anson	Duncan Whitfield
Final 3.0			
3.1	Update post titles and holders and department name	Jo Anson	

Distribution / Actions

Name	Job Title	Action
	Departmental Records Managers	For comment

Nathan Cooper	Head of Data Security (Contractor)	For review & comment
Tom Crisp	Senior Lawyer	For review & comment
Jo Anson	Head of Financial and Information Governance	For review and comment
CGP		For review & comment

Final distribution

This policy is available to all Southwark employees and Council members through The Source. Hard copies for distribution may be requested through the Information Governance Manager.

1 Introduction

In collecting, processing, sharing and disposing of personal information relating to living individuals, Southwark Council is bound by the Data Protection Act 1998 (the Act). This Act came into force on 1 March 2000. It repealed the Data Protection Act 1984, the Access to Personal Files Act 1987 and most of the Access to Health Records Act 1990. The Information Commissioner's Office enforces the Act, issues relevant guidance and registers data controllers.

This document sets out Southwark Council's policy for compliance with the Data Protection Act (DPA). Procedures for responding to requests are outlined in the Guidance on handling Data Protection Requests.

Review of this policy

This policy will be reviewed, at least, on a two yearly basis to ensure that it takes account of new legislation and expected developments in the areas of personal privacy and public sector data sharing.

1.1 Rights and General Principles

The Act creates a single framework for access to personal information about living persons held in both paper and electronic form. It enhances the rights of data subjects in that it confers a general right of access. There are seven rights under the Act:

1. **The right to subject access:** This allows people to find out what information is held about them.
2. **The right to prevent processing:** Anyone can ask a Data Controller not to process information relating to them that causes substantial unwarranted damage or distress to them or anyone else.
3. **The right to prevent processing for direct marketing:** Anyone can ask a Data Controller not to process information relating to him or her for direct marketing purposes.
4. **Rights in relation to automated decision taking:** Individuals have a right to object to decisions made only by automatic means e.g. there is no human involvement.
5. **The right to compensation:** An individual can claim compensation from a Data Controller for damage and distress caused by any breach of the act. Compensation for distress alone can only be claimed in limited circumstances.
6. **The right to rectification, blocking, erasure and destruction:** Individuals can apply to the court (or the Information Commissioner) to order a Data Controller to rectify, block or destroy personal details if they are inaccurate or contain expressions of opinion based on inaccurate information.
7. **The right to ask the Commissioner to assess whether the Act has been contravened**

There are also eight data protection principles which are shown in Appendix D.

Southwark Council is a registered Data Controller under the Act and will comply with these.

2 Roles and Responsibilities

2.1 Senior Information Risk Manager SIRO

The SIRO, currently the strategic director of finance and governance:

- is ultimately accountable for the assurance of information security at the council
- is the champion of information security at chief officer level
- owns the corporate information security policy
- acts as chief knowledge officer,
- oversees compliance with the Act, and areas advises on relevant matters to help ensure compliance by the council.

2.2 Monitoring Officer

The monitoring officer, currently the director of legal services, will be responsible for:

- ensuring compliance with the Act
- coordinating responses to the Information Commissioner's Office.

2.3 All Chief Officers

All chief officers, for their directorates, will be responsible for:

- Ensuring appropriate technical and organisational measures are taken against unauthorised or unlawful processing and against accidental loss or destruction of personal data.
- Ensuring compliance with this policy and any associated procedures in the processing of personal information.
- Ensuring all breaches are reported and appropriately dealt with.

2.4 All Managers

Business unit managers or delegated officers are responsible for:

- Maintaining awareness of data security and monitoring the application of data security policies and protocols.

.

2.5 Data Security Manager

The data security manager has responsibility for:

- Overall responsibility within the council for the development and management of all aspects of data and information security.
- Ensuring the council's compliance with statutory and regulatory requirements.
- The effective management and application of the council's risk assessment, audit, business continuity and disaster recovery as they apply to the council's systems and IT.
- Input to the on-going development and implementation of the IS strategies, policies and initiatives to ensure the security of systems and data.
- Maintaining a log of all data security breaches
- Overseeing and reporting any significant breaches in security to senior management and implements any required remedial action.

2.6 The Information Governance Manager

The information governance manager will act as the council's data protection officer:

- Provide advice across the council on all Data Protection issues
- Draft guidance on handling requests made under the Act
- Manage the information governance team.

2.7 The Corporate Information Governance team

The information governance team has responsibility for:

- Maintaining notification to the Information Commissioner's Office on behalf of the monitoring officer
- Logging and monitoring the volume of Subject Access Requests and ensuring compliance
- Escalating complex cases as necessary to the monitoring officer.

2.8 Caldicott Guardians

Caldicott Guardians are officers appointed by the council to have responsibility for ensuring that client and patient data is kept secure both within the council and when being transferred to other bodies.

The council has appointed the following officers as its Caldicott Guardians:

- Jon Newton, Acting Head of Quality & Transformation, Children's and Adults Services
- Jackie Cook, Head of Social Work Improvement and Quality Assurance, Children's and Adults Services

See appendix A for information about the Caldicott principles.

2.9 Elected Members

Elected members may process personal data in several capacities and their responsibility will reflect this:

- As members of the council they may have access to and process personal data in the same way as employees. The data controller is the council rather than the elected member. An example is of a member of a housing committee who has access to tenancy files for the purpose of considering whether or not the Council should proceed with an eviction. In this case the elected member is not required to notify.
- When councillors act on their own behalf, they are Data Controllers in their own right of this information; members services register all elected members as data controllers. Examples include the processing of personal data in order to timetable surgery appointments or progress complaints made by local residents. When campaigning within their own political parties for adoption as a prospective candidate for a particular ward they also act as individuals and can only rely upon the notification of their parties if as a matter of fact the parties control the manner and the purpose of the processing of personal data for the purpose of their individual campaigns.

- When acting on behalf of a political party, however, for instance as an office holder or as an official candidate, members are entitled rely upon the data protection notification made by the party.
- Elected members should be aware that they need to arrange for appropriate security to protect personal information. They must take into account the nature of the information and the harm that can result. They should consider what technical measures and organisational measures, such as use of passwords, computer access privileges, procedures and staff training, are appropriate to keep the information safe. Elected members should seek advice from member services, the data security manager or the information governance team.

2.10 Employees

The council holds information about service users, local residents, elected members and employees, among others. Everyone who works for or represents the council must protect the personal data that they use and be aware of their obligations. The use of personal data must be fair, legal and proportionate.

Staff cannot use personal data obtained at work for their own purposes. It is a criminal offence knowingly or recklessly to disclose personal data without the council's permission. Anyone who uses, discusses or discloses personal data held by the council without lawful authority may commit this offence, the penalty for which is up to two years in prison.

Staff who knowingly disclose or misuse council data for their own purposes, or who knowingly ignore the requirements of this policy will face disciplinary action, regardless of any possible criminal sanction. This could lead to dismissal in some cases.

Employees when working at home must take all reasonable precautions to protect information and data relating to their work from loss or damage and in accordance with the Homeworking guidelines

Employees can be considered members of the public in terms of the right to make Subject Access Requests. However, as members of staff they have responsibility to:

- Process personal information in compliance with the eight Data Protection principles
- Make personal information available to Data Subjects following a valid Subject Access Request (according to the Request Handling Procedures).

Employees' responsibilities for applying the legislation are set out in paragraph 3 below; including security (3.10) and the transfer of data (3.14). All staff must be aware of the actions they can and cannot take, seeking clarification from their manager where necessary.

3 Applying legislation

3.1 Processing Personal Data

Southwark Council will process data in accordance with the Data Protection Principles.

Processing under the Act is defined as:

"Processing", in relation to information or data, means obtaining, recording or holding the information or data or carrying out any operation or set of operations on the information or data, including-

- organisation, adaptation or alteration of the information or data,
- retrieval, consultation or use of the information or data,
- disclosure of the information or data by transmission, dissemination or otherwise making available, or
- alignment, combination, blocking, erasure or destruction of the information or data;

Southwark Council, when processing personal data, will adhere to the following Principles:

- only collect data necessary to carry out the defined function that the task relates to and only hold and process personal data for the purposes of undertaking its statutory functions
- respond to requests for access to personal data within 40 days (requests must be provided in writing)
- only withhold information where exceptions under the Act permit.
- treat all personal information with equal respect for confidentiality and security whether in written, spoken or electronic form.
- seek consent to the sharing of personal or sensitive data, unless doing so would interfere with other statutory requirements, such as law enforcement.
- only retain personal data for a specified time period defined by the Southwark Retention Schedule.
- not delay data sharing where it is necessary for Southwark Council to protect the vital interests of a data subject, a minor or another person
- only use third parties to collect and process data where they can ensure confidentiality of data subjects' information and operate according to the eight principles under the Act.
- collect and process employee data in accordance with the Act and with The Employment Practices Data Protection Code issued by the Information Commissioner.

3.2 Conditions for Processing Personal Data

Schedule 2 of the Act describes a list of conditions, at least one of which must be met before personal information can be processed fairly and lawfully:

- The Data Subject has given their consent to the processing.
- The processing is necessary
  - for the performance of a contract to which the Data Subject is a party, or
  - for the taking of steps at the request of the Data Subject with a view to entering into a contract.

- The processing is necessary for compliance with any legal obligation to which the Data Controller is subject, other than an obligation imposed by contract
- The processing is necessary in order to protect the vital interests of the Data Subject.
- The processing is necessary
  - for the administration of justice
  - for the exercise of any functions conferred on any person by or under any enactment
  - for the exercise of any functions of the Crown, a Minister of the Crown or a government department, or
- The processing is necessary for the purposes of legitimate interests pursued by the Data Controller or by the third party or parties to whom the data are disclosed, except where the processing is unwarranted in any particular case by reason of prejudice to the rights and freedoms or legitimate interests of the Data Subject.

3.3 Conditions for Processing Sensitive Personal Data

Schedule 3 of the Act provides an additional list of conditions, at least one of which must also be met before sensitive personal data can be processed fairly and lawfully.

- The Data Subject has given their explicit consent to the processing
- The processing is necessary to perform any legal right or obligations imposed on the organisation in connection with employment
- The processing is necessary to protect the vital interests of the individual or another person, where consent cannot be given by the individual, or the organisation cannot be reasonably expected to obtain consent or consent is being unreasonably withheld where it is necessary to protect the vital interests of another
- The information contained in the personal information has been made public as a result of steps deliberately taken by the individual
- The processing is necessary in connection with legal proceedings, dealings with legal rights or taking legal advice
- The processing is necessary for the administration of justice or carrying out legal or public functions
- The processing is necessary for medical purposes

Consent to collect sensitive personal data will be obtained by providing a comprehensive notice of the intended purpose(s) for which the sensitive personal data will be processed, together with an opt-in tick box or signature box by which the data subject can clearly indicate their consent for this data to be processed as described.

3.4 Awareness and training

The council will promote the need to respect privacy and confidentiality so that people remain confident about using council services. To do so, the council will provide basic data protection training for all employees, including temporary employees.

3.5 Obtaining information

People must be informed when we record information about them, unless there is a specific legal reason for not doing so. Any process involving the collection and use of personal data must conform to the DPA principles. Managers must ensure that the use of personal data

meets these conditions. People must be told how we will use their data, so that they are not reluctant to provide it to us.

3.6 New processes and services

Departments need to know the legal basis for using and sharing personal data as defined in the Data Protection Act 1998 when developing a new service or process. The relevant department will, where necessary, carry out a Privacy Impact Assessment (PIA) on new initiatives or existing services or projects, and in any case where the impact of the change is significant or intrusive. The PIA will identify any areas of concern within a new project which relate to information governance issues and ensure that they are put right before the project begins.

If we need consent to use personal data, we will obtain it as soon as possible. If consent is not required, we will still tell people how their data will be used.

3.7 Application forms and tools to gather information

Any form or process designed to gather information must include a simple explanation about why personal data is needed, and what we will do with it. This 'fair processing notice' (as directed by the Data Protection Act) must also spell out whether data will be shared outside the council. Existing forms without fair processing information will be amended when it is practical to do so.

3.8 Notification

The council's 'notification', which is held by the Information Commissioner and is available from the Information Commissioners Office (ICO) website describes how and why we use personal data; it is reviewed annually. Departments should tell the information governance team about new services or projects, or significant changes that might affect the notification (see also 3.6).

The member services team will process notifications on elected members' behalf.

3.9 Record keeping

Departments must put in place adequate records management procedures, including measures to ensure that working records about people are fair, accurate, up-to-date and not excessive. Records about people must be secure, traceable and accounted for at all times. Records must be disposed of securely in accordance with the retention schedule. Records management procedures, including retention and disposal, apply equally to paper and electronic records including emails.

3.10 Security

All premises and electronic systems where personal data is held must have adequate security. Access to areas where information is held should be controlled, paper files containing personal data must be locked away when not in use, and computer data must be protected by adequate security measures. Access to data should be restricted to authorised staff only; such staff should receive training on the security of the system prior to being allowed access to it.

Where information is gathered and recorded through mobile working then staff should download the data onto the appropriate network server as soon as possible. Personal data should not be stored on unencrypted devices.

All staff must ensure that when dealing with the public, clients should not have access to screens or data on which other clients records are displayed or can be seen.

Care should be taken if personal data is used outside the office environment, whether it is on paper or in a computer file. Departments should have in place systems whereby account is kept of who takes personal data off the premises and when it is returned.

Lockable containers should be provided for personal data if it is used outside the office environment and these should not be left on view in vehicles.

Data must not be stored on any equipment owned by members of staff including, but not limited to, mobile phones, MP3 players, cameras, memory sticks, home computers, tablets or laptops.

Personal data should not be emailed to employees' home computers, as working from home should be through secure remote access.

Electronic data must only ever be stored on official servers. If this is impractical, data must be only stored in locations agreed by the Head of Data security.

It is council policy to store data on a network server where it is regularly backed up.

All valuable files, client personal information and documents must be stored on the appropriate server on the council's network and not on Desktop PCs or laptops or other electronic storage devices. Information stored on Desktop PCs and laptops etc. is at risk of loss through hardware or software failure or automated administrative activity, or loss or theft of equipment.

If in exceptional circumstances, data is not stored on the network then it is the responsibility of users to ensure that the data is secure and appropriate back-up procedures are operated. Managers must approve this and data must be downloaded appropriately as quickly as possible after the event and deleted from the mobile storage device.

All data, physical or electronic, must be disposed of securely, in accordance with the council's retention policy. Equipment which may record equipment electronically must be decommissioned in accordance with the council's policy. Note that printers and photo copiers may record personal data.

3.11 Extent of information

Personal data must be accurate, relevant, up-to-date, adequate and not excessive. It should be easy for staff and service users to update their data. Inaccuracies must be corrected as soon as they come to light. Staff should ensure that they keep enough information to provide an effective service, but avoid keeping data just in case it may become useful in the future.

3.12 Need to know

Access to personal data must only be available to those who need it. Data should be used when necessary and not purely because it is convenient to do so. Each department is responsible for restricting access to personal data and ensuring compliance. This applies to all staff, including ICT staff and non-technical staff with 'administrator' or similar status. All access to systems containing personal data for maintenance or testing must be logged. Where a system has the facility to log the creation of users, this facility must be switched on.

3.13 Validating requests for information

Departments must understand the legal framework that affects their work, so that they know when they have the power or the obligation to disclose information to other organisations, and to obtain it from them.

If an outside body requests personal data from the council, staff must take reasonable steps to check the identity and entitlement of the person requesting it. Requests for information should be made in writing to make clear what is required. If an outside body says they can demand personal data held by the council, the legal basis of that right must be checked. For more information see the Guidance on handling Data Protection Requests.

3.14 Security of transfer

Information should be shared by the most secure method available. When sending information outside the council, staff must take steps to ensure that only appropriate people will see it.

In some cases the most appropriate method for sharing data will be by using the Government Secure Intranet (GSI) Staff can send data using this secure infrastructure by requesting a Government Connects Secure Extranet (GCSx) account. The GCSx is a secure network that allows officials at local public-sector organisations to interact and share data privately and securely with central government departments, such as the Department for Work and Pensions, the National Health Service, the Criminal Justice Extranet and the Police National Network.

When using GCSx staff must ensure that all documents sent over GCSx are given the appropriate protective marking

If email is considered to be the best option, staff must use the correct email address and be aware that email inboxes may be monitored by managers or others who may not be entitled to access personal data. Emails should therefore be marked as confidential. Consideration should be given to whether to data being transferred requires encryption. The same applies to fax transmission. If you are sending encrypted files, you must call the recipient and verbally communicate the password to them. If you are unable to reach the recipient by telephone, or a telephone call is impractical for other reasons, email the recipient and ask them to contact you to confirm receipt of the data. You can then send the password in a separate email. Do not send the password in the same email as the encrypted file.

Staff can ensure that data is sent to them securely by using the secure mail facility provided by the Criminal Justice System. Your secure email address is the same as your usual email address but with a “cjsm.net” extension at the end, for example

first.last@southwark.gov.uk.cjsm.net

john.person@southwark.gov.uk.cjsm.net

Sensitive data should not be sent by email unless steps have been taken to ensure that the recipient is not forwarding mail to another inbox, or that the inbox is not being monitored.

3.15 Information Sharing

An information-sharing agreement or protocol is not a legal requirement to share information – sharing can happen without one. An agreement does not create a legal gateway if one does not already exist. However the use of a protocol will ensure best practice by all partners in any information sharing partnership.

All agreements or protocols between the council and outside agencies must be notified to the information governance manager. Departments must not sign an agreement without seeking advice from either the information governance manager or the council’s legal services section. Agreements should be drawn up after consultation between organisations, not imposed on by one another. Any agreement must comply with the Caldicott Principles to ensure that confidentiality is safeguarded.

Any information sharing should be carried out using the risk assessment process and the Information Commissioner’s guidance.

Non-sensitive personal data provided to the council may be shared across departments and services within the council, and contractors employed by the council, for the purposes of:

- Recovering sums owed to the council: rent and service charges, contractual payments, charges for the provision of any facility or service, application fees, fines, costs, or in respect of the recovery of any grant or overpayment made by the council.
- Updating council records
- Preventing and detecting fraud

In the case of sensitive personal information the council will make every effort to obtain informed consent from the data subject. Consent assumes communication between the Southwark Council and the data subject and this may be through discussion, however, evidence of consent should then be obtained and held. Failure by the data subject to return a form requesting consent will not be assumed by the council to imply consent. In some cases, it may be necessary to disclose without consent, in order to protect the vital interests of the data subject, or other person or where it has not been possible to obtain consent, see 3.3 above.

.

3.16 Contracts

If a contract or agreement involves the sharing of personal data, the contract should include measures to ensure that the data is used safely and appropriately. Information supplied to contractors can only be used for agreed purposes, and must not be used or disclosed for any other reason without further consultation with the council.

3.17 Induction

Information about confidentiality and data protection must be provided to all new members of staff prior to them having access to the council's network and any personal data and all new staff should be signposted towards the basic data protection training e-learning module.

3.18 Privacy Impact Assessments (PIAs)

When starting any new substantial project every attempt should be made to ensure that the privacy of the client information involved is respected and that all systems are compliant with the Human Rights Act and the Data Protection Act. In order to ensure this, it is necessary to conduct a PIA. These assessments are defined by the Information Commissioner as processes whereby a project's potential privacy issues and risks are identified and examined from the perspectives of all stakeholders, and a search is undertaken for ways to avoid or minimise privacy concerns. As in 3.6, these assessments will involve the risk assessment for any new project which deals with personal data. When any new system is considered the information governance manager must be informed.

3.19 Confidentiality

Information explicitly accepted in confidence or as part of a confidential relationship can only be disclosed to someone else in exceptional circumstances. Employees must not disclose confidential information to anyone else without the permission of the individual who first gave the information to them, unless the information is about serious wrong-doing or harm.

All staff have a duty to report any criminal activity or wrong doing to the proper authorities if they become aware of them. The council operates a Whistleblowing Policy, which provides further advice on what to do in these situations; this policy is on the council's intranet.

Elected members should be aware of the provision of the Members' Code of Conduct regarding confidential information and also this policy if the information contains personal data.

3.20 Testing and training

When developing or testing any new system or process or working on an existing system for the purpose of testing or training then data about real people must not be used unless it is

impossible to test the system without live data. This applies to staff or contractors when testing or upgrading systems. If live data must be used for testing, the data must be secure, and not accessed or disclosed unless strictly necessary. Inconvenience is not sufficient reason to use live data for testing.

Personal data must not be used in any training exercise – real examples must be fictionalised to the point where a person cannot be identified. Personal data can only be used for training purposes where managers or supervisors need to discuss with an officer the way they handled a specific case or situation.

3.21 Procedure for data loss

The data security manager and the council's legal services team must be notified of any actual loss, theft or accidental disclosure of personal data.

The data security manager and the council's legal services team will ensure proper investigation of the loss, evaluation of the risks involved and mitigation of those risks.

The data security manager and the council's legal services team will determine whether a serious breach has occurred and will recommend to the monitoring officer and chief knowledge officer whether a breach should be reported to the Information Commissioner.

Although there is no legal obligation on data controllers to report breaches of security which result in loss, release or corruption of personal data, the Information Commissioner believes serious breaches should be brought to the attention of his Office.

4 Subject Access Requests

Data subjects have a right of access to information about themselves that includes factual information, expressions of opinion, and the intentions of Southwark Council in relation to them, irrespective of when the information was recorded. Southwark Council will disclose any information they hold on a data subject (applying any necessary exemptions) within 40 calendar days of receiving a valid Subject Access Request.

Alternatively, service users may request access to their case files directly from the relevant business unit, for example, area housing offices or social services. After verifying the data subject identity, access will be facilitated by the business unit in accordance with Schedule 2 and 3 of the Act. However **all** such requests will be notified to the information governance team.

4.1 Proof of Identity

To protect the data subject and avoid disclosing data to unauthorised persons the council will require proof of identification and address from the requester prior to releasing the data. Such proof must be hand delivered; however, in circumstances where this is not practicable alterative arrangements will be determined on a case by case basis. For more information see the Guidance on handling Data Protection requests.

4.2 Requests from advocates

Data subjects can also make a request for information through a representative or agent such as a solicitor; such representatives must have the written consent of the data subject. The council will ask for proof that consent from the data subject has been received, and for proof of identification of the Data Subject and Advocate. A record of this consent must be held on file. For more information see the Guidance on handling Data Protection requests.

4.3 Requests relating to employees

Southwark Council, in accordance with the Information Commissioner's guidance will disclose information identifying council employees and ex-employees acting in their official capacity of council officer, such as name, job title and work phone number. Therefore, if a third party organisation or individual, such as a contractor has provided information to the council in carrying out its business function for and on behalf on the council, this information is eligible for disclosure.

4.4 Processing Subject Access Requests

Subject Access Requests should be submitted to the information governance team for logging and processing:

By post:
Corporate Freedom of Information Officer:
Information Governance team
PO Box 64529
London

SE1P 5LX

By email: accessinfo@southwark.gov.uk

Data Subjects should:

Describe as precisely as possible the information they wish to access, including where relevant:

- Date of birth

- Any previous addresses within the borough they have lived in and
- List of service areas they think may hold information about them
- Any previous names they may have had

Requests for personal information will be processed as outlined in the Guidance on handling Data Protection requests.

4.5 Minors and People with Learning Disabilities

The Act makes no special provisions in relation to requests made by adults, children, people with learning disabilities, or a mental disorder. Southwark Council will administer the Gillick Competence test (see Appendix) in assessing a Subject Access Request to determine if the data subject has the required mental capacity in understanding the implications of allowing access to their records.

4.6 Persons lacking mental capacity

A person may lack the mental capacity, that is, the ability to understand information and make an informed decision. In line with the Mental Capacity Act 2005 every effort should be made to assist a person in decision making and this includes understanding and giving consent for the disclosure and sharing of information about them. Consideration should be given to whether the decision needs to be made immediately or whether the person will be able to understand the nature of an information request at a later date.

The Mental Capacity Act 2005 creates a Lasting Power of Attorney (LPA) that enables individuals to appoint others to act on their behalf in decision making situations when they are not able to do so. The LPA for welfare matters comes into force when the individual is deemed to lack capacity for whatever welfare or care decision is being made. The LPA also grants the holder a right of access to information. The normal process dictated by the DPA and as detailed above should be followed when dealing with such an access request and in addition we would normally ask to see a copy of LPA before we disclose the information.

Once it is deemed the person concerned lacks capacity and it is deemed in the best interests of the person to share information the holder of the LPA will be required to provide a copy of the LPA papers to ensure the council is satisfied it will meet its statutory requirements.

The LPA must be registered with and stamped by the Court of Protection. More information can be sought from The Office of the Public Guardian http://www.publicguardian.gov.uk/ It should be noted that this is not an express right to have access to the full record of another, only what is considered relevant material and deemed to serve the best interests of the person should be disclosed.

For those individuals who may lack capacity and family members who do not hold an LPA, decisions about information sharing should always be considered under best interest principles.

5 Fees

Southwark Council reserves the right to charge the statutory fee of £10 for Subject Access Requests. Southwark Council also reserves the right to apply fees as specified by other relevant legislation.

The current policy at Southwark Council is not to levy a fee for any Subject Access requests.

6 Complaints and Role of the Information Commissioner

In the event of a complaint regarding the Subject Access request including application of an exemption, the initial request, decision audit trail, correspondence and information released will be reviewed independently of the original decision maker by an appropriate council officer consistent with the council's scheme of delegation.

All complaints will be notified to the information governance team for logging.

If the requester is dissatisfied with the complaint outcome they may seek an independent review by the Information Commissioner. The Information Commissioner has the authority to demand disclosure.

Southwark Council will comply with all notices and guidance issued by the Information Commissioner.

Appendix A Caldicott Principles

The December 1997 Caldicott Report identified weaknesses in the way parts of the NHS handled confidential patient data. The report made several recommendations, one of which was the appointment of Caldicott Guardians, members of staff with a responsibility to ensure patient data is kept secure, and identified six principles underpinning information governance.

The Department of Health asked Dame Fiona Caldicott to carry out a review of information governance. Her report was published in April 2013 and revised the existing principles and added a seventh. These are set out below:

- Principle 1 – **Justify the purpose(s)**
  Every proposed use or transfer of patient-identifiable information within or from an organisation should be clearly defined and scrutinised, with continuing uses regularly reviewed by an appropriate guardian.
- Principle 2 – **Don't use patient-identifiable information unless it is absolutely necessary**
  Patient-identifiable information items should not be used unless there is no alternative.
- Principle 3 – **Use the minimum necessary patient-identifiable information**
  Where use of patient-identifiable information is considered to be essential, each individual item of information should be justified with the aim of reducing identifiability.
- Principle 4 – **Access to patient-identifiable information should be on a strict need to know basis**
  Only those individuals who need access to patient-identifiable information should have access to it, and they should only have access to the information items that they need to see.
- Principle 5 – **Everyone with access to personal confidential data should be aware of their responsibilities**
  Action should be taken to ensure that those handling patient-identifiable information - both clinical and non-clinical staff - are aware of their responsibilities and obligations to respect patient confidentiality.
- Principle 6 – **Comply with the law**
  Every use of patient-identifiable information must be lawful. Someone in each organisation should be responsible for ensuring that the organisation complies with legal requirements.
- Principle 7 – **The duty to share information can be as information as the duty to protect patient confidentiality**

  Sharing information can be in the best interests in the patient if it is done within the framework set out in these principles and is in line with the policies of employers, regulators and professional bodies.

Appendix B Gillick Competence

The rights of parents in relation to medical matters concerning their children are subject to the ruling of the House of Lords in the case Gillick v West Norfolk and Wisbech Area Health Authority [1985] 3 All ER 402 (HL).

The case concerned a teenage child's right to consent to medical treatment without the parents' knowledge. Lord Fraser said that the degree of parental control varied according to the child's understanding and intelligence, and Lord Scarman further opined that parental rights only existed so long as they were needed to protect the property and person of the child. He said:

> *"As a matter of law the parental right to determine whether or not their minor child below the age of 16 will have medical treatment terminates if and when the child achieves sufficient understanding and intelligence to enable him to understand fully what is proposed."*

Subsequently developed case law held that 'Gillick competence' related to the particular child and the particular treatment, and there have been cases where a 17-year-old has been found insufficiently competent to refuse medical treatment, while in other cases much younger children have been deemed sufficiently competent. In addition, where a child is 16 or 17 either parent or child can consent to treatment independently (though neither can override the other or exercise a veto). The court can, however, override the wishes of both where treatment is vital to the child's welfare.

Attempts by medical professionals to further clarify the law were specifically discouraged by the courts. It became a matter for the doctor to judge whether a child under 16 was 'Gillick competent'.

A further anomaly was provided by the Access to Health Records Act 1990, which allows a child under 16 deemed 'Gillick competent' by a doctor to veto the parent's access to medical information held by that doctor, even though the parent can consent to treatment which the child cannot veto.

The result is that a doctor, if s/he judges the child to be 'Gillick competent', can only disclose information to the parent with the child's consent, regardless of Parental Responsibility.

If a person does not have the capacity to manage their affairs, a person acting under an order of the Court of Protection or who has Enduring Power of Attorney can request access on her or his behalf. People with learning disabilities or mental health problems do not necessarily lack the mental capacity to make a subject access request on their own behalf. Such requests require a judgement to be made on a case-by-case basis as to their mental capacity.

Appendix C Glossary

Data Subject	A living individual to whom the Personal Data relates (e.g. Service Users, Clients, and Employees).
Data Controller	A term that describes those who collect and use Personal Data; in this case Southwark Council.
Information Commissioner	Responsible for implementation and policing of the Data Protection Act and the Freedom of Information Act, with the authority to investigate and prosecute.
Personal Data	Any information – held manually or electronically – which relates directly to a Data Subject. This can include: Name and Address, Date of Birth, Qualifications, Income level, Employment history
Sensitive Personal Data	Personal data under the following headings: a) Race or ethnic origin b) political opinion c) religious or other beliefs d) trade union membership e) physical or mental health condition f) sexual orientation g) details of offences, court sentences or allegations under investigation
Processing	Organising, adapting and altering data; retrieval, consultation or use of the data in any way; blocking or erasing data. It even includes glancing at a computer screen and disclosure to anyone within or outside the Council.

Appendix D The Data Protection Principles

Southwark Council is a registered Data Controller under the Act and will comply with the eight principles defined as:

1 Information should be processed fairly and lawfully.

2 Personal data shall be obtained for one or more specified and lawful purpose and shall not be processed in any manner incompatible with that purpose.

3 Personal data shall be adequate and relevant and not excessive.

4 Personal data should be accurate and up to date.

5 Personal data should only be kept as long as necessary.

6 Personal data shall be processed in accordance with the rights of data subjects under the Act.

7 Appropriate technical and organizational measures shall be taken against unauthorised or unlawful processing and against accidental loss or destruction.

8 Personal data should not be transferred to a country outside the European Union unless that country has an adequate level of protection for the rights and freedoms of the data subject.