Title: Data Protection Policy v6

Key Points:

- Somerset Partnership NHS Foundation Trust (SPFT) is defined as a data controller and as such all Staff, Contractors and Volunteers have a responsibility for data protection.

- Data protection applies to all the personal and “sensitive” special category data held by, and on behalf of the SPFT. This information must be lawfully and fairly processed and where required explicit consent must be obtained and recorded.

- You must only access personal data, client records, files and folders which you “need to know” in order to do your job. Unauthorised access is a criminal offence.

- Safeguarding of people, at immediate risk of harm, over-rides data protection concerns.

- All members of the public and employees, as data subjects, have statutory rights including the right to know what information we hold and to have a copy of that information.

- You must complete the Annual Information Governance training.

- You must report any suspected data breach of personal or sensitive data to the Information Governance Team within 72 hours of becoming aware of the breach.

- Make yourself aware of the additional statutory responsibilities, including the need for Privacy Notices, Data Processing Agreements, Records Management, Data Protection Impact Assessments and the SPFT Data Protection Officer.
1 Policy Statement

Somerset Partnership NHS Foundation Trust (SPFT) will ensure every user is aware of, and understands, their responsibilities regarding the security of personal data held by, and on behalf of, SPFT in respect of:

- their responsibilities under data protection law for the protection of personal data
- the benefits of appropriate data sharing
- the necessity for good records management
- the technical and administrative controls operating at SPFT
- other laws and statutory guidance around this subject

2 Purpose

SPFT collects, holds and uses personal data in order to conduct its business. SPFT has a statutory duty under the UK data protection legislation and related statutes to safeguard this information. This data covers, but is not restricted to, the following:

- Patients and members of the public
- Current, past and prospective employees
- Partners, Suppliers and Contractors

In addition, it may occasionally be specifically required by law to collect and use certain types of personal information to comply with the requirements of government departments such as the Police the Council, DWP and other 3rd parties.

This policy outlines every user’s responsibilities in respect of Data Protection and signposts users to detailed policy and guidance in particular areas.

3 Scope

This policy is intended for all Committees, Trustees, Services, Partners, Employees of SPFT, Contractual Third Parties and Agents of the Trust who has access to information held or processed by SPFT.

This policy covers all personal information held by SPFT however it is collected, recorded and used, whether digital, on paper or recorded on other media.

This document describes the policies for correctly handling personal and special category data in order to comply with the current data protection legislation and related statutes.

This policy relates to all personal data collected by SPFT.

4 Definition

This document defines the policy, practice and procedure to ensure the security of personal and sensitive information held by SPFT.

SPFT will adhere to the current data protection legislation, and other relevant statutes and protocols. It will implement the controls recommended for by Data Security and Protection Toolkit and where practical apply the principles promoted by the Cyber Essentials Plus and ISO 27001:2013 framework.
SPFT will ensure that all Committees, Trustees, Services, Partners, Employees of SPFT, Contractual Third Parties and Agents of the Trust who have access to any information held by or on behalf of SPFT are fully aware of, have received training in, and abide by, their duties and responsibilities under current legislation and guidance. [ICO Data Protection Guidance]

5 Risks

SPFT recognises that there are risks associated with users accessing and handling personal information in order to conduct official Trust business.

This policy aims to mitigate the risks associated with breaches to the data protection legislation. There are a variety of risks some of which can culminate in the Information Commissioner’s Office (ICO) imposing significant fines.

- inappropriate access to personal records
- the loss or theft of personal & sensitive data
- lack of effective and safe data sharing
- inadequate records management
- inadequate destruction of data
- not carrying out data protection impact assessments (DPIA)
- not publishing notification to data subjects of their rights
- inadequate processing of Data Subject Access Requests (DSARs)

Non-compliance with this policy could have a significant effect on the efficient operation of SPFT and may result in reputational damage, financial loss, ICO fines and an inability to provide necessary services to our customers.

6 Applying the Policy to the Data Protection Legislation

6.1 Principles relating to processing of Personal Data - Article 5

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 considered to 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 that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay (‘accuracy’);

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) The controller shall be responsible for, and be able to demonstrate compliance with, paragraph 1 (‘accountability’)

6.2 Legal Bases for Processing Personal Data – Article 6

Processing shall be lawful only if and to the extent that at least one of the following applies:

a) the data subject has given consent to the processing of his or her personal data for one or more specific purposes;

b) processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract;

c) processing is necessary for compliance with a legal obligation to which the controller is subject;

d) processing is necessary in order to protect the vital interests of the data subject or of another natural person;

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;

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.

6.3 Legal Bases for Processing Special Category Data – Article 9

Processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person’s sex life or sexual orientation shall be prohibited.

The above shall not apply if one of the following applies:

a) 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;

b) 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;
c) 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;

d) processing is carried out in the course of 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;

e) processing relates to personal data which are manifestly made public by the data subject;

f) processing is necessary for the establishment, exercise or defence of legal claims or whenever courts are acting in their judicial capacity;

g) 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;

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

i) processing is necessary for reasons of public interest in the area of 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, in particular professional secrecy;

j) 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 the interests of the data subject.

6.4 Transparency, Privacy Notices and advising data subjects of their rights

The SPFT privacy notice describes to the general public how the Trust processes personal data. It is published on the internet on this link SPFT Privacy Notice and an appropriate version should be available to all data subjects in SPFT offices where personal data is collected in the form of posters and / or leaflets.

If you regularly collect information in forms, questionnaires or surveys, your documentation must include the Privacy Notice with provision for ensuring you have a statutory right to process the personal data by law, under contract or via another suitable legal basis appropriate to the purpose.

If you regularly collect personal information over the phone ensure the script you read to the patient includes the option for a data subject to be informed of their rights under data protection law.
6.5 Data Protection Impact Assessments (DPIA)

SPFT must carry out a Data Protection Impact Assessment (DPIA) in all decision making processes and projects where personal and special category data is used. SPFT DPIA Policy is published on the intranet.

6.6 Information Control and Compliance

The methods by which data is managed and controlled within the organisation, need to ensure that data is effectively shared and protected whilst at rest and in transit.

6.7 Data Subject Rights

6.7.1 The right to be informed

Individuals have the right to be informed about the collection and use of their personal data.

6.7.2 The right to access records – Subject Access Request (SAR)

The public can request to see all the data that the SPFT holds about them or someone they have a legal responsibility for. SPFT Subject Access Procedure is published on the intranet.

6.7.3 The right to request rectification – the correction of incorrect information

If a data subject identifies that information we hold about them is incorrect SPFT must investigate and if the law allows correct the error. However, in many cases SPFT will be required to keep the old record by law and will instead append a note to the record advising of the suggested correction.

6.7.4 The right to request erasure / deletion of their records (right to be forgotten)

A data subject can request that we delete records we hold about them. However, in the majority of cases SPFT will be required to keep the record by law and will instead append a note to the record advising that the request was made but declined.

6.7.5 The right to restriction – restricting the processing of personal data

When a data subject requests that we rectify or delete records we hold about them we are obliged to cease processing the record. However, in the majority of cases SPFT will be required to continue processing the record by law and will instead append a note to the record advising that the request was made but declined.

6.7.6 The right to portability

A data subject can request that we transfer their personal data records to another data controller in a machine-readable form. This is highly unlikely to occur in normal Trust business and only applies to electronic records.

6.7.7 The right to object to processing

A data subject can object to SPFT processing their personal data and we could be obliged to do this. However, in the majority of cases SPFT will be required to continue processing the record by law and will instead append a note to the record advising that the request was made but declined.
6.7.8 **The right to object to automated decision making & profiling**

A data subject should not be subject to automated decision making unless authorised by UK law or if SPFT has explicit consent. As SPFT does not in general use profiling or automated decision making unless it is acting under statute this is again unlikely to apply.

6.7.9 **The right to complain to the Information Commissioner’s Office**

If a data subject has cause for complaint about how their personal data has been processed by the Trust or one of our partners / contractors they must be advised of their right to complain to the Information Commissioner’s Office (ICO). SPFT must provide them with full contact details for the ICO.

6.8 **Information Security - Acceptable Use Policy**

SPFT must protect personal data across a wide range of technologies and in a variety of environments. The Information Security Policy describes how each aspect of this is managed and your responsibilities for keeping personal and sensitive data secure.

Only access personal data which you need to know in order to do your job.

6.9 **Post**

SPFT must consider the risks of sending out all documents and consider if any additional safeguards are required to protect the information being sent.

Documents must be classified according to their sensitivity, the volume of data they contain, the destination or recipient of the data. All these factors will influence the decision on the postal service used, the packaging to protect the information and the cost of delivery.

6.10 **Fax machines**

Fax should not be used to transmit personal and sensitive information except as a method of last resort or in an emergency. Fax machines carry greater risk than email with regard to accidental disclosure;

- outside SPFT, due to incorrect dialling
- inside SPFT, if information is picked up or read by the wrong person

Fax machines catering for personal and sensitive data should not be located in the common way areas or on corridors. If a fax machine has to be used the risk of disclosure can be mitigated by:

- setting fax machines with auto-dial for regular recipients
- checking that any fax auto-dial is correct for the recipient
- ensuring that a trusted recipient is waiting at the other end of the fax line
- sending a preliminary test page to check that the fax number is correct
- marking each page with the ‘page X of Y’ function to check the entire document is sent

6.11 **Recording of meetings**

Unless there is an overriding safeguarding concern, or an instruction from the Courts a patient cannot legally be prevented from recording a meeting with SPFT employees.
However, in order to mitigate the risk of unauthorised disclosure of personal data the chair of the meeting, or the SPFT Representative present should remind the attendees;

- that the meeting is confidential and ask if anyone is recording the meeting
- that under the GDPR/DPA 2018 any recording can only be used for "domestic purposes" and must not be used on social media
- that any disclosure may harm the current and/or future interests of a vulnerable person
- that any disclosure of 3rd party personal information requires their consent
- that Courts may consider covert recordings inadmissible

6.12 Mobile phones and SMS messaging

For the purposes of this policy smartphones and standard mobile phones will all be called "mobile phones".

The personal data that could be held on mobile phones will be in the form of Contacts, Calendar Appointments, corporate email, personal email, photographs, text messages and messages sent using “apps”.

Users must not store personal data relating to SPFT patients or clients on a personal mobile phone unless it is protected by Mobile-iron. If you are using a corporate smartphone or if you are using a personal phone, with Mobile-iron installed, all the personal data held by SPFT will be encrypted.

To mitigate the risks should your mobile phone be lost or stolen, you must ensure you:

- have a timeout on the screen to lock it out
- have a password to lock the phone, preferably 8 digits mixed alpha-numeric
- only store essential data on the phone
- only keep data on the phone for a short period

6.13 Phone calls / Skype

When making a phone call or using Skype for calls of a personal and sensitive nature:

- ensure you cannot be overheard by anyone not directly concerned with the call
- before sharing personal data ensure the other party is a trusted individual, if necessary call them back to confirm their identity
- outside the office ensure you cannot be overheard by anyone, where this is not possible try only first names and try and avoid discussing personal and sensitive issues

6.14 Email

In order to perform their duties SPFT provides individual access to email via a centrally managed service.

Confidential information regarding patient and staff, or other individuals, must not be sent externally via email unless encrypted.

SPFT provides an encryption facility using WatchGuard. Type the word “(ENCRYPT)” in brackets and the message will be automatically encrypted to the recipient.
Users need to note that statements made in emails must be factual and truthful and do not contain, for example gossip. Where incorrect statements are made about individuals and companies, SPFT is potentially liable.

It is permissible for staff to send and receive email during breaks for incidental personal purposes provided that doing so does not involve a substantial expenditure of time or is used for profit.

All suspected infringements will be considered on a case by case basis.

Staff are encouraged to use the Outlook ‘out of the office’ rule when they are on leave or unable to check their email for more than one day. This enables the sender to seek an alternative response to the message they have sent.

Staff must not permit another person to access and use their email address unless previously authorised for legitimate working practices for example proxy access for a PA to a Manager’s or Consultant’s account.

Staff must not encourage or promote any activity that is unlawful or illegal.

Care needs to be taken when addressing messages as it is easy when using distribution groups to circulate an email more widely than intended.

Users must ensure that information circulated via email complies with copyright law.

Automated forwarding of email to another account must be restricted to internal email addresses. Email must never be forwarded to any personal or external email accounts.

Do not open attachments unless you are sure they are from a trusted source. Treat external attachments with caution and check the nature and purpose of the attachment with the sender.

Viruses and other malicious software are often sent as attachments and for this reason, some attachments may be quarantined to ensure the safety and security of the Trust network.

All emails created from SPFT managed systems are the property of the Trust and the Trust retains the right to access email accounts should misuse of the facility be suspected.

6.15 Overarching Tier 1 Data Sharing Protocols

SPFT recognises the need to share personal and sensitive data with other partner organisations in order to provide effective care and services.

SPFT has overarching Universal Data Sharing Protocols agreed with the Council, the Police and other local NHS organisation to assist in the design of individual agreements with partner agencies. Please ensure that if the agreement is initiated by the other party that it contains all the elements contained within this Protocol.

6.16 Information Sharing Agreements (ISA’s)

If you intend to set up a service or change a service that will necessitate the sharing of personal or sensitive data with another data controller or data processor you must have an Information Sharing Agreement in place.
6.17 Contract Clauses

If you intend to set up a service or change a service that will necessitate the sharing of personal or sensitive data with a private sector data controller or data processor, such as a contractor, you must have the correct contract clauses in place similar to the ones below. The Procurement Service can advise on how this should be done.

6.18 Data Processing Agreement

If you intend to set up a service or change a service that will necessitate the processing of personal or sensitive data by another organisation, such as an IT contractor, you must have a Data Processing Agreement in place.

6.19 Data Transfers

If you intend to transfer personal or sensitive data to a third party or contractor you must have the data transfer approved by the SPFT Information Governance (IG) Team. Before approving the transfer the IG team will consider:

- the sensitivity of the data
- the volume of data to be transmitted
- the security offered by the third party
- the country to which the data is to be sent

6.20 Records Management

The SPFT Record Keeping and Records Management Policy concerns the lifecycle of information from creation to destruction. Records should be created, stored, processed, accessed and destroyed in adherence to the Principles of the GDPR and DPA 2018, the Records Management Code of Practice for Health and Social Care and the statutory ICO Code of Practice that regulates Records Management.

The policy is applicable to all records held by staff on computers and in offices across the Trust, and not only those held in the records stores and archives. This policy includes guidance on Data retention, the applicable retention schedules and secure data destruction.

6.21 Use of CCTV

SPFT operates a range of CCTV cameras across the Trust for the purposes of Prevention & Detection of Crime, Health & Safety and Traffic Management. These cameras are situated on some buildings and at key road junctions and exits.

6.22 Data Breaches & Security Incidents

If you are aware that you, or someone else, has disclosed personal or sensitive data, to someone who did not have permission or authority to receive that information, you must report it immediately to the Information Governance Team within 72 hours:

- If any personal information has been sent to the wrong individual, in paper form, attempts must be made to recover the information, ideally in person.
- If any personal information has been sent to the wrong individual, in electronic form, attempts must be made to ensure the recipient has deleted the information from their computer and email.
• Complete an incident reporting form in line with the Trust’s Untoward Event Reporting Policy and Procedure. On receipt the Information Governance team will ensure they have all the necessary information in case the breach needs to be notified to the Information Commissioner’s Office (ICO) within 72 hours.

The mandatory process that governs how that data breach is dealt with is covered in detail in the Untoward Event Reporting Policy and Procedure.
Policy Compliance

If any employee is found to have breached this policy, they may be subject to Somerset Partnership NHS Foundation Trust’s Disciplinary Procedure.

Where it is considered that a criminal offence has potentially been committed, SPFT will consider the need to refer the matter to the police.

If you do not understand the implications of this policy or how it may apply to you, seek advice from the Information Governance Team.

Policy Governance

The following table identifies who within Somerset Partnership NHS Foundation Trust is Accountable, Responsible, Informed or Consulted with regards to this policy. The following definitions apply:

- **Responsible** – the person(s) responsible for developing and implementing the policy.
- **Accountable** – the person who has ultimate accountability and authority for the policy.
- **Consulted** – the person(s) or groups to be consulted prior to final policy implementation.
- **Informed** – the person(s) or groups to be informed after policy implementation.

<table>
<thead>
<tr>
<th>Responsible</th>
<th>Data Protection Officer</th>
</tr>
</thead>
<tbody>
<tr>
<td>Accountable</td>
<td>SIRO – Director of Strategic Development</td>
</tr>
<tr>
<td>Consulted</td>
<td>Data Security and Protection Group, Delivery Group, HR</td>
</tr>
<tr>
<td>Informed</td>
<td>All Staff, (substantive, bank or honorary), Students and Volunteers</td>
</tr>
</tbody>
</table>

Review and Revision

This policy will be reviewed as it is deemed appropriate, but no less frequently than every 24 months.

References

Somerset Partnership NHS Foundation Trust policy documents that are directly relevant to this policy, are referenced within this document:

Legislation

- The General Data Protection Regulation 2018
- The Data Protection Act 2018
- The Computer Misuse Act 1990
- The Human Rights Act 1998
- The NHS Confidentiality Code of Practice 2003
- The NHS Act 2006: Section 251
- The Access to Health Records Act 1990
- The Mental Capacity Act 2005