THE STATE HOSPITALS BOARD FOR SCOTLAND

INFORMATION GOVERNANCE
DATA PROTECTION (GDPR) POLICY

Policy Reference Number	IG05	Issue: 8
Lead Author	Information Governance and Data Security Officer	
Contributing Authors	Finance & eHealth Director	
	Members of the Information Governance Group	
Advisory Group	Information Governance Group	
Approval Group	Policy Approval Group	
Implementation Date	24/06/2021	
Next Review Date	24/06/2024	
Accountable Executive Director	Finance & eHealth Director	

The date for review detailed on the front of all State Hospital policies/ procedures/ guidance does not mean that the document becomes invalid from this date. The review date is advisory and the organisation reserves the right to review a policy/ procedure/ guidance at any time due to organisational/legal changes.

Staff are advised to always check that they are using the correct version of any policy/ procedure/ guidance rather than referring to locally held copies.

The most up to date version of all State Hospital policies/ procedures/ guidance can be found on the intranet: http://intranet.tsh.scot.nhs.uk/Policies/Policy%20Docs/Forms/Category%20View.aspx

REVIEW SUMMARY SHEET

No changes required to policy (evidence base checked)	☐

Changes required to policy (evidence base checked) ☒

Summary of changes within policy:

Front Page - Title changed to include (GDPR)

Introduction / Purpose - was updated to change EU GDPR to UK GDPR and to show the split between GDPR and law enforcement purposes

Scope - changed to exclude law enforcement purposes

4.7 Information Asset Owners(IAO) - Sight change to the definition (due to TSH having and IAO that isn't a director and added the responsibility to negotiate information sharing agreements

5. Special Categories of Personal Data - added Criminal conviction and criminal offences information

6.2.1 Notification – Changed section title from registration to reflect current requirements. Changed responsibility from DPO to SIRO and added a paragraph on IAO's required to notify IAO about changes to the use of data.

7.4 Disciplinary issues – Updated wording regarding the deliberate or reckless breaching of policy or law.

10.1 Content – Added transfers outside of the UK.

10.2 Responsibilities – removed "creation and" from the line "The DPO is responsible for the creation and maintenance of the Information Asset Register."

12.1 – 12.4 – changed 30 days to one calendar month.

12.4 Rights to Object to Processing – changed "process" to "processing" twice

12.7 Rights of Access – Changed "to a third country" to "outside the UK"

13. Transfers of personal data outside the United Kingdom (UK) – Changed section name to replace EEA with UK.

14. Breaches of Personal Data – updated text to include notifying the data subject.

Appendix A – Added IG15 Privacy Impact Assessment Guidance

Contents

1. Introduction / Purpose

The Data Protection Act 2018 (DPA) and the UK General Data Protection Regulation (GDPR) imposes obligations on the use of all personal data held by The State Hospital, whether it relates to patients and their families, employees, complainants, contractors or any other individual who comes into contact with the organisation. This has implications for every part of the organisation.

The State Hospital and its employees are bound by a legal duty of confidentiality to all data subjects which can only be set aside to meet an overriding public interest, legal obligation, or similar duty.

The legislation applies to all staff, contractors and volunteers working for The State Hospital.

The State Hospital is a Controller, as defined in Article 4 of the GDPR, and is obliged to ensure that all of the DPA and GDPRs' requirements are implemented.

This policy, IG05 Data Protection (GDPR) Policy, sets out how The State Hospital meets its legal obligations and requirements under confidentiality, data protection and information security standards for processing personal information for purposes other than law enforcement.

Where The State Hospital has a statutory function for a law enforcement purpose, The State Hospital is a 'competent authority' as defined by Section 30(1)(b) of the DPA and as a Controller, as defined in Section 32 of the DPA.

IG22 Data Protection (Law Enforcement) Policy sets out how The State Hospital meets its legal obligations and requirements under confidentiality, data protection and information security standards for processing personal information for purposes of law enforcement.

Law enforcement purposes are the purposes of prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security.
The chief requirements outlined in this policy are based upon the DPA and GDPR, which are the central pieces of legislation covering security and confidentiality of personal information.

This policy should be read in conjunction with The State Hospital's other Information Governance policies, procedures and guidance listed in Appendix A.

A summary of other legislation and guidelines relevant to this policy is found in Appendix B.

2. Legislative Framework

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

The DPA specifically identifies health, housing, education and social work records as "accessible records", which means that all electronic data and manual data from any of these categories meets the definition of personal data (even if that manual data is not stored in a relevant filing system).

The use of personal information for law enforcement purposes is specifically governed by part 3 of the DPA whereas almost all other uses of personal information are governed by the GDPR.

All personal data must be handled according to the DPA and the GDPRs' requirements, and this policy contributes to how this is delivered.

3. Scope

This policy applies to all staff, contractors and volunteers at The State Hospital, when they are processing personal information for purposes that are not a law enforcement purpose.

4. Management and Responsibilities

4.1 The Controller.

The State Hospital as Controller is obliged to, taking into account the nature, scope, context and purposes of processing personal data, implement appropriate technical and organisational measures to ensure and demonstrate that processing is performed in accordance with data protection legislation.

This includes;

- Implementation of appropriate data protection policies and procedures.
- Adherence to codes of conduct or approved certification mechanisms approved by the Information Commissioner's Office (ICO).
- Ensuring that the policies and procedures are designed to, by default, only process personal data that is necessary for each specific purpose.
- Measures shall ensure that by default personal data is not accessible to an indefinite number of people without the individual's intervention.

4.2 Chief Executive

The Chief Executive has overall responsibility for Data Protection within The State Hospital.

Information Sharing Agreements will be signed on behalf of The State Hospital by the Chief Executive.

The Director of Nursing and Allied Health Professions deputises in the absence of the Chief Executive.

4.3 Senior Information Risk Owner (SIRO)

The SIRO is responsible for coordinating the development, implementation and maintenance of information risk management policies, procedures and standards for The State Hospital. It is their role to:

- Oversee the development and implementation of this policy and a strategy for implementing the policy.
- Take ownership of risk assessment process for information risk including review of risk assessments carried out on Information Assets.
- Review and agree action in respect of identified information risks.
- Ensure that The State Hospital's approach to information risk is effective in terms of resource, commitment and execution and that this is communicated to all staff.
- Provide a focal point for the resolution and/or discussion of information risk issues.
- Ensure executive management is adequately briefed on information risk issues.

The Finance and Performance Management Director is designated as The State Hospital's SIRO.

The Chief Executive or a person nominated by the Chief Executive deputises in the absence of the Finance and Performance Management Director.

4.4 Data Protection Officer (DPO)

The State Hospital is required to appoint a suitably qualified Data Protection Officer. Their role is to:

- Provide The State Hospital, its employees, contractors and volunteers with advice and guidance regarding their obligations under data protection legislation.
- Monitor compliance of data protection legislation with regard to The State Hospital's policies and procedures, assignment of responsibilities, awareness and training of staff, and related audits.
- Provide advice were requested regarding privacy impact assessments and the monitoring of their performance.
- Cooperate with the supervisory authority in relation to data protection matters. The UK supervisory authority is The Information Commissioner's Office (ICO).
- Manage Subject Access requests.
- Act as a contact point for data protection matters.

The monitoring of compliance with this policy and related procedures is delegated to The DPO.

The Information Governance and Data Security Officer is designated as The State Hospital's DPO.

The Health Records Manager deputises in the absence of the Information Governance and Data Security Officer.

4.5 The Caldicott Guardian

The Caldicott Guardian has responsibility for advising Hospital staff and ensuring adequate arrangements be put in place to protect patient identifiable information.

The Associate Medical Director is designated as The State Hospital's Caldicott Guardian.

The Medical Director deputises in the absence of the Associate Medical Director.

4.6 The Information Governance Group (IGG)

The members of the Information Governance Group are responsible for overseeing the development of this policy and its implementation. The IGG on behalf of the Caldicott Guardian are responsible for ensuring the effective integration of respective policies for control of patient identifiable information and on behalf of the SIRO for staff identifiable and any other identifiable information held on suppliers etc. The group on behalf of The State Hospital are also responsible for ensuring the following:

- Each individual is aware of their rights
- Delivery of staff and patient awareness and training in relation to this policy
- Delivery of Information Governance to meet national standards
- Production of the IGG Annual Report which is presented by the Caldicott Guardian to the Clinical Governance Committee

4.7 Information Asset Owner (IAO)

IAO are the directors of the hospital and individuals designated by the Chief Executive. They are owners for one or more identified information assets. The State Hospital's IAOs are required to:

- Ensure the confidentiality, integrity, and availability of all information that their system processes and protect against any anticipated threats or hazards to the security or integrity of such information.

- Undertake privacy impact assessments and information risk assessments on all information assets where they have been assigned 'ownership', following guidance from the DPO on assessment method, format, content, and frequency.
- Negotiate Information Sharing Agreements with other stakeholders where needed prior to seeking Chief Executive sign off.
- Supply reports on measures taken to mitigate or deal with information risks to the IGG
- Authorise changes to user access arrangements for the asset.
- Provide information from their assets to fulfil subject access request.
- Provide a suitably qualified individual to support subject access redaction procedures.
- Promptly report any suspected or actual breaches of data protection to the DPO.

Each IAO must ensure that there is a suitable deputy to cover planned and unplanned absence.

4.8 Information Asset Administrator (IAA)

An IAA is a member of staff nominated by an IAO to manage an information asset on a day to day basis on their behalf.

IAA responsibilities will vary depending on the IAO's needs and the requirements of the information asset. These may include:

- Managing user access to the asset.
- Being a first point of contact for the asset.
- Extracting information for Subject Access requests.
- Performing redaction as part of the Subject Access procedure.

4.9 Managers

All managers are responsible for ensuring that this policy is communicated and implemented within their area of responsibility. They are responsible for the quality, security and management of personal data in use in their area and promptly report any suspected or actual breaches of data protection to the DPO via DATIX.

Advice or assistance regarding this policy or data protection in general is available from the DPO.

4.10 All Staff, Volunteers and Contractors

Everyone has a role in the effective management of risk, including information risk. All staff must actively participate in the process of information risk management by:

- following The State Hospital procedures regarding the handling of personal data
- identifying and reporting potential information risks in their area
- handling and sharing information responsibly at all times

All data protection and information security related incidents should be **promptly** reported via DATIX.

4.11 Provisions for Continuity and Resilience

The State Hospital will make provision by way of designated personnel; to ensure that there is adequate cover to maintain data protection functions in the event of planned and unplanned absences of:

- The Chief Executive
- The Senior Information Risk Owner
- The Data Protection Officer

- The Caldicott Guardian
- Information Asset Owners

5. Special Categories of Personal Data

Certain types of personal data are considered to be particularly sensitive and processing them is prohibited without additional conditions being met. These are known as 'Special categories' of personal data.

Special categories of data are:

- Personal data that reveals a data subject's racial or ethnic origin, political opinions, religious or philosophical beliefs.
- Data relating to a data subject's genetics, sex life and sexual orientation.
- Data concerning health.
- Biometric data with is processed to the purpose of uniquely identifying a data subject.
- Criminal convictions and criminal offences information

6. Data Protection Principles

The GDPR contains 6 principles which regulate the use of personal data. The principles apply to all personal data, however it might be obtained.

6.1 Personal data shall be processed fairly, lawfully and transparently.

(GDPR Article 5(1)(a))('Lawfulness, fairness and transparency')

The State Hospital is obliged to meet specific criteria before processing personal data, and to make the public aware of how it uses personal data, and to ensure that they are properly informed with whom their data is shared.

6.1.1 Data subjects (Patients, Staff and Third Parties)

Data subjects must be made aware of how their data will be used by The State Hospital directly. When information is requested from data subjects verbally or using an application form, a clear explanation should be provided about how the data will be used. Data subjects can also be informed by the use of privacy policy information leaflets, either provided directly or made available in data subject areas. Where appropriate, information posters in waiting areas, and privacy statements in handbooks/on survey forms might also be used.

6.2 Personal data shall be obtained for specified and lawful purposes, and shall not be further processed in any manner incompatible with those purposes.

(GDPR Article 5(1)(b))('Purpose limited')

6.2.1 Registration

The State Hospital is required to register annually with the Information Commissionaire's Office.

The SIRO is responsible for ensuring the annual registration to the ICO is accurate and maintained.

6.2.2 Incompatible re-use of information

IAOs should notify the DPO if personal data is to be used for a different purpose than that for which it was obtained. This is to ensure that re-uses of information are not incompatible with the original purpose for which the data was obtained.

6.3 Personal data shall be adequate, relevant and limited in relation to the purpose or purposes for which they are processed.
(*GDPR Article 5(1)(c))('Data minimisation')*

IAOs should ensure that any data collected from individuals is complete, and the level of data retained on The State Hospital's systems is required for current, existing purposes, and sufficient to support appropriate and effective decisions.

6.4 Personal data shall be accurate and, where necessary, kept up to date
(GDPR Article 5(1)(d))('Accuracy')

IAOs must ensure that personal data held on any media is accurate and up to date. The State Hospital will via procedures and operational protocols manage validation routines to promote accuracy of information.

Users of software are responsible for the quality (i.e. accuracy, timeliness, completeness) of their data by carrying out their own quality assurance and participating as required in quality assurance processes.

Personal information should also be checked for accuracy on a regular basis

6.5 Personal data processed for any purpose or purposes shall not be kept for longer than is necessary for that purpose or those purposes.
(GDPR Article 5(1)(e))('Storage limitation')

Personal data must not be retained indefinitely, and IAOs must ensure that they are aware of, and compliant with The State Hospital's management, retention and disposal policies for administrative and clinical records.

6.6 Personal data shall be processed in a manner that ensures appropriate security of the personal data.
(GDPR Article 5(1)(f))('Integrity and confidentiality')

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

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

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

6.6.1 Information Security

The eHealth department is responsible for ensuring that systems under the control of The State Hospital and The State Hospital's users comply with current Data Protection legislation. This includes responsibility for ensuring that procedures are in place to achieve a high level of data quality.

This includes ensuring that:

- users are set up on the system on a need to know basis
- IAO have been advised of their responsibilities and carried out a risk assessment on the asset for which they are responsible, in accordance with The State Hospital's Risk Management procedures.
- advice is sought from the DPO regarding Data Protection issues whenever appropriate, and Data Protection implications are considered at the earliest stage whenever systems are procured or altered
- disclosures of information are checked and appropriate
- unusual requests for disclosure must be scrutinised and referred to the IAO / DPO when necessary
- eHealth staff must be aware of their responsibilities regarding security, data protection and confidentiality issues

6.6.2 Back-ups

eHealth are responsible for ensuring there are procedures which outlines the media, frequency and retention period for back-ups of the data and programs for the systems within their control.

Those systems which are 'run' for the users by eHealth will have their systems backed up on a regular basis. The master copy of programs and back-ups of data will be kept in a fireproof data safe, ideally in a separate building or off site from the system.

6.6.3 Information in Transit

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

Where possible, sensitive categories of personal data should be sent in a digital format using an encrypted medium. (I.e. To an NHS email address, on an encrypted CD, etc.)

The transport of personal data via encrypted CDs can be done using a signed for delivery service.

6.6.4 Data Processors

Where The State Hospital uses a contractor to process personal data on its behalf, the contractor must sign a data processing agreement which ensures that they are taking adequate steps to comply with the processing instructions and data protection legislation on behalf The State Hospital. The State Hospital retains legal responsibility for the actions of processors, and so those managing contracts must ensure that they contact the DPO to ensure that security procedures are specified in the contract, and subsequently checked to ensure that they are in place.

Contracts between The State Hospital and third parties must include an appropriate confidentiality clause which should be disseminated to the data processor's employees.

7. Staff Awareness

7.1 Training

The State Hospital has a mandatory training programme which includes maintaining awareness of data protection, confidentiality and security issues for all staff. This is carried out by annual computer based training sessions covering the following subjects:

- personal responsibilities
- confidentiality of personal information
- relevant State Hospital Policies and Procedures
- compliance with the Data Protection Principles
- individual rights
- general good practice guidelines covering security and confidentiality
- records management

7.2 Induction

All new starters are given standard Information Governance training as part of The State Hospital's induction process. Additional training in these areas will be given to those who require it due to the nature of their job. A register will be maintained of all staff attendance at training sessions.

7.3 Contracts of Employment

Staff contracts of employment are produced and monitored by The State Hospital's Human Resources department. All contracts of employment include a data protection and general confidentiality clause. Agency and contract staff are subject to the same rules.

7.4 Disciplinary issues

All personal data recorded in any format must be handled securely and appropriately, and staff must not disclose information for any purpose outside their normal work role.

It is a criminal offence to deliberately or recklessly disclose personal data without permission from The State Hospital.

Any unauthorised or reckless disclosure of information by a member of staff will be considered as a disciplinary issue.

8. Children and Young People

8.1 Consent and confidentiality

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

8.2 Consent - young people aged 16 and 17

Young people aged 16 or 17 are presumed to be competent for the purpose of consent and are therefore entitled to the same duty of confidentiality as adults.

8.3 Consent - children 13 - 16

Children between the ages of 13 and 16, who have the capacity and understanding to take decisions about their own affairs, are also entitled to make decisions about the use and disclosure of information they have provided in confidence.

In other cases, consent should be sought from a person with parental responsibility if such a person is available.

8.4 Information Sharing without consent

The sharing of information about children and young people should generally happen under the same principles that apply to adults. The default position is that information should be shared with consent; where information sharing is required and consent cannot be obtained (or asking for it would be inappropriate), the individual should still be informed.

There may be circumstances where consent cannot be obtained or where it would obviously be refused. Decisions about sharing in these circumstances should be made in the best interests of the child or young person.

Disclosure without consent may be justified:

- Where the young person does not have sufficient understanding to appreciate what the advice being sought may involve.
- Where the young person cannot be persuaded to involve an appropriate person in a discussion or consultation that is in their best interests.
- Where it would be essential to the best interests of the data subject.

8.5 Safeguarding

Sharing of information between practitioners is essential to ensure that children are properly protected. Information from different sources may have to be put together to ensure that a child can be identified as being in need or at risk of harm. Where there are concerns that a child is, or may be at risk of significant harm, the professional must follow The State Hospital Child Welfare / Protection Procedure for Reporting Concerns.
(http://intranet.tsh.scot.nhs.uk/GroupsCommittees/ChildandAdultProtectionForum/Documents/Child%20Protection%20Reporting.pdf)

9. Data Protection by Design

The State Hospital is obliged to implement appropriate technical and organisational measures to ensure that, by default, only personal data which are necessary for each specific purpose are processed. These measures shall ensure that by default personal information is not made available to an indefinite number of people.

The State Hospital will implement a ‘Privacy by Design’ procedure that requires a privacy impact assessment and as appropriate, consultation with stakeholders to ensure all processing of personal information is conducted in accordance with legislation.

10. Information Asset Register

The State Hospital will create and maintain a register of all information assets that utilise personal data that it has responsibility for as Controller.

10.1 Content

The register must record at least the following information.

- The name of the asset
- The purpose(s) of the asset
- The Information Asset Owner
- The types of personal data held in the asset

- Any special categories of data held in the asset
- The legal justification for processing.
- Categories of recipients that the data will be disclosed to.
- The retention period of the data
- The date the asset was created
- The date the asset was closed
- The method of privacy notice used to inform the data subject.
- A review date
- Copies of all Privacy Impact Assessments for the asset
- The security arrangements for access to the asset
- Transfers outside the UK, the name of the country and the legal safeguards
- Any special instructions. (I.e. access rights/ destruction requirements, etc.)

10.2 Responsibilities

The DPO is responsible for the maintenance of the Information Asset Register.

IAOs are responsible for providing the required information, privacy impact assessments and risk assessments for the registration of the asset.

IAOs must ensure that any changes to the use of the asset are promptly reflected in the Information Asset Register.

10.3 Disciplinary issues

Operation of an information asset that is not registered in the Information Asset Register is a breach of data protection legislation that could result in a member of staff facing disciplinary action.

11. Privacy Notices

When personal data is obtained by The State Hospital it is necessary to inform the data subject about it. The State Hospital will use privacy notices to comply with this requirement.

11.1 Personal Information obtained from the data subject

Where personal data is obtained from the data subject, The State Hospital shall, at the time of collection provide a privacy notice that includes;

- The identity and contact details for The State Hospital or their representative
- The contact details of the DPO
- The purpose for processing the personal data
- The legal basis for processing
- The recipients or categories of recipients of the personal data
- Where applicable, the fact The State Hospital intends to transfer the personal data to a third country and the existence or absence of suitable safeguards.
- The retention period for the information, or the criteria used to determine the period.
- The existence of rights to request from The State Hospital;
  - access to their personal data
  - rectification of their personal data
  - erasure of their personal data
  - restriction in processing their personal data
- The right to object to the processing of their personal data

- The right to data portability.
- Where ‘consent’ has been used as the legal basis to process, the right at any time to withdraw consent.
- The right of the data subject to lodge a complaint with the ICO
- Whether the collection of information is a statutory or contractual requirement, or a requirement to enter into a contract, as well as any obligation on the data subject to provide the information and the possible consequences of failing to do so.
- Where applicable, the existence of automated decision-making, including profiling and meaningful information regarding the logic involved. The significance and envisaged consequences for the data subject.

Where The State Hospital intends to further process personal data for a purpose other than the purposes given at collection, then The State Hospital will provide a privacy notice to the data subject prior to the additional processing occurring.

11.2 Personal Information not obtained from the data subject

Where personal data is not obtained from the data subject, The State Hospital shall provide a privacy notice, within one month of collection, or at the first communication or at the first disclosure of the information, whichever is the earliest.

In addition to the privacy notice in section 11.1 the data subject should be informed;

- The source of the data and if applicable, whether it came from a public source.

Where The State Hospital intends to further process personal data for a purpose other than the purposes given at collection, then The State Hospital will provide a privacy notice to the data subject prior to the additional processing occurring.

12. Data Subject Rights

Data protection legislation provides a number of rights to data subjects. When a data subject exercises any of their rights, the DPO and the IAO should be notified immediately.

12.1 Rights to Rectification

A data subject has the right, without undue delay, to:

- rectification of inaccurate personal data,
- complete personal data that is incomplete

It is the responsibility of an IAO to ensure that documented procedures are in place to facilitate the correction and completion of personal data within one calendar month of notification.

12.2 Rights to Erasure

A data subject has the right, without undue delay, to the erasure of their personal data where any of the following apply:

- The personal data is no longer necessary for the purpose it was collected for.
- The data subject withdraws consent AND where there are no other legal grounds for processing.
- The data subject objects to the processing AND there are no overriding legitimate reasons for processing.
- The data subject objects to the processing of direct marketing

- The personal data has been processed unlawfully.
- The personal data has to be erased for compliance with a legal obligation.

It is the responsibility of the IAO to ensure documented procedures are in place to facilitate the erasure of personal data within one calendar month of notification. The IAO should seek guidance from the DPO prior to commencing any erasures.

12.3 Rights to Data Portability

Where a data subject has given consent to the processing of their personal data by automated means, they may require The State Hospital to provide the data in a structured, commonly used and machine-readable format, and that the data is transferred to another Controller without hindrance.

It is the responsibility of the IAO to ensure documented procedures are in place to facilitate the packaging and transfer of personal data within one calendar month of notification. The IAO should seek guidance from the DPO prior to commencing any transfers.

12.4 Rights to Object to Processing

Data subjects have the right to object to the processing of their personal data where:

- The legal basis for processing is consent
- The legal basis for processing is necessary for the performance of a task carried out in the public interest
- The purpose of processing is direct marketing.

Unless The State Hospital has compelling legitimate grounds which override the interests, rights and freedoms of the data subject or is in the pursuit of legal claims, then The State Hospital shall stop processing the data.

It is the responsibility of the IAO to ensure documented procedures are in place to facilitate the cessation of processing personal data within one calendar month of notification.

12.4.1 Direct Marketing

The State Hospital is obliged to cease sending correspondence for the purposes of direct marketing if an individual indicates that they no longer wish to receive it. The ICO's definition of direct marketing is "the offer for sale of goods and services, and the promotion of an organisation's aims and ideals". Staff should be aware that correspondence sent to influence decisions or choices is likely to be covered by this definition.

12.5 Rights in Relation to Automated Processing

Data subjects have the right not to be subject to a decision based solely on automated processing that produces a legal or similar significant effect on them unless:

- It is necessary from the performance of a contract, or
- It is required by law, or
- It is based on the data subject's explicit consent.

Where automated processing occurs under contract or consent, it is the responsibility of the IAO to ensure that there are documented procedures in place to permit the data subject to obtain human intervention to express their views and contest the decision.

12.6 Rights to Restrict Processing

A data subject has the right to obtain a restriction of processing personal data where any of the following apply:

- Where the accuracy of the data is contested by the data subject, a restriction for a period of time to enable The State Hospital to verify the accuracy of the data.
- Where the processing is unlawful and the data subject opposes the erasure of their personal data, a restriction can be used.
- Where the information is no longer needed by The State Hospital, but the data subject requires the data for a legal claim.
- Where the data subject is objecting to an automated decision-making process, a restriction for a period of time to enable The State Hospital to verify whether the legitimate grounds used by The State Hospital overrides those of the data subject.

When a restriction to process personal data is in force, the only activities permitted are:

- Storage & backup.
- Any processing agreed the data subject with their consent.
- Any processing pursuant to a legal claim.
- Any processing for the protection of the rights of another.
- Any processing for reasons of important public interest.

If any restriction is enacted, the data subject must be informed by The State Hospital BEFORE the restriction is lifted and processing resumes.

It is the responsibility of the IAO that documented procedures are in place to enable restriction of process to be managed for their asset. Any request to restrict processing should be notified to the DPO.

12.7 Rights of Access

A data subject has the right to obtain from The State Hospital confirmation as to whether or not personal data relating to them is being processed, and, where that is the case, access to the following information:

- The purposes of the processing
- The categories of personal data being processed
- The recipients or categories of recipients that data has been or will be disclosed.
- The retention period of the data or the criteria used to determine the retention period.
- The existence of the right to request rectification, erasure and restriction of processing personal data.
- The existence of the right to object to processing of personal data.
- The right to lodge a complaint with the ICO
- The source of any personal data not collected from themselves.
- The existence of any automated decision-making and the logic involved.

Where personal data is transferred outside the UK, a data subject has the right to be informed of the appropriate safeguards relating to the transfer.

It is the responsibility of the IAO to ensure documented procedures are in place to supply this information.

12.7.1 Subject Access Requests

Individuals have a right to request any personal data held by The State Hospital in whatever form.

The State Hospital has a Subject Access Request procedure to manage requests for access to information – in summary, all subject access requests must be sent to the DPO for processing.

The Access to Health Records Act 1990 provides access rights to a deceased person's representatives if they are making a claim. These should also be sent to the Caldicott Guardian

It is the responsibility of the IAO to ensure documented procedures are in place to support the Subject Access Requests Procedure.

12.8 Notifications Regarding Rights

When a data subject exercises their rights to any rectification, erasure or restriction then The State Hospital has an obligation to communicate such to all recipients of the information, unless this is impossible or involves disproportional effort.

The DPO is responsible for communicating to recipients the exercising data subjects rights' where practical.

12.9 Complaints

The State Hospital's complaints procedures take account of complaints which may be received because of a breach or suspected breach of the Data Protection Act 2018 or GDPR. Individuals should be advised of The State Hospital's complaints procedures if they are unhappy about the way in which their data has been used.

13 Transfers of personal data outside the United Kingdom (UK)

Anyone who wishes to send person identifiable information in any format to outside the UK, must discuss this with the DPO as the levels of protection for the information may not be as comprehensive as those in the UK. In the majority of cases, such sharing will only be possible with the specific consent of the individuals whose data is to be shared.

14. Breaches of Personal Data

A breach of personal data may occur when personal information is used in ways that have not been agreed by The State Hospital through the Privacy by Design process in section 9.

The State Hospital is obliged to report personal data breaches to the data subject where the breach has a high risk to their rights and freedoms, without undue delay. More serious breaches also require notification to the ICO.

The DPO will provide advice to The State Hospital regarding the severity of the breach and if notification is required.

Notification to the ICO should be within 72 hours of The State Hospital becoming aware of a notifiable breach.

14.1 Recording of Personal Data Breaches

All data protection and information security related incidents shall be recorded, documenting the facts relating to the incident, its effects and any mitigation taken.

DATIX is the recording system for The State Hospital.

Where an incident is complex a supplementary record may be held by the DPO.

14.2 All Staff

All data protection and information security related incidents should be **promptly** reported via DATIX. When recording a potential incident staff should use 'Communications/Information Governance' as the type of incident.

14.3 Notification to the DPO

All suspected personal data breaches must be reported to the DPO via DATIX.

14.4 Investigation of Personal Data Beaches

Investigations into potential breaches of personal data should be conducted promptly using the hospital's risk management procedures for investigating incidents.

Investigators should liaise with the DPO to ensure that any external notifications requirements are met.

14.5 Notification to the Data Subject

Where a breach of personal data has occurred and there is a high risk to the rights and freedoms of a data subject The State Hospital will, without undue delay, inform the individual in clear and plain language:

- of the nature of the breach
- the contact details of the DPO
- the likely consequences of the breach
- the measures taken by The State Hospital to address the breach

14.5.1 Exceptions to Data Subject Notification

Notification to the data subject will be at The State Hospital discretion in cases where the hospital:

- had appropriate measures in place that means that the information is unintelligible to unauthorised viewers, such as encryption
  Or
- has subsequently taken steps to ensure that the high risks to data subject are no longer likely to materialise.

Where notification to the data subject would involve a disproportionate effort then a public communication or similar measure can be used.

14.6 Notification to the ICO

The State Hospital is obliged to report personal data breaches to the ICO without undue delay.

Notification should be within 72 hours of the breach occurring unless notification would prejudice the rights and freedoms of an individual.

In the event of notification exceeding 72 hours, a written explanation of the delay must be included in the notification.

The DPO is responsible for notifying the ICO of any such breaches.

15. Format

The State Hospitals Board recognises the need to ensure all stakeholders are supported to

understand information about how services are delivered. Based on what is proportionate and reasonable, we can provide information / documents in alternative formats and are happy to discuss with you the most practical and cost effective format suitable for your needs. Some of the services we are able to access include interpretation, translation, large print, Braille, tape recorded material, sign language, use of plain English / images.

If you require information in another format, please contact the Person Centred Improvement Lead on 01555 842072.

16. Stakeholder Consultation

Key Stakeholders	Consulted (Y/N)
Patients	N
Staff	Y
TSH Board	Y
Carers	N
Volunteers	N

17. Communication, Implementation, Monitoring and Review of Policy

This policy will be communicated to all stakeholders within The State Hospital via the intranet and through the staff bulletin. The Advisory Group will be responsible for the implementation and monitoring of this policy. This policy will be reviewed every three years, and when appropriate to take into account changes to legislation that may occur, and / or guidance from the Government and/or the ICO.

Appendices

Appendix A – The State Hospital's IG Policies, Procedures and Guidance

IG01 Freedom of Information Policy
IG02 Health Records Policies and Procedures
IG03 Management Retention Disposal of Admin Records
IG04 External Website Maintenance Development Policy
IG05 Data Protection Policy (This Policy)
IG06 Intellectual Property Policy
IG07 Intranet Maintenance and Development
IG08 Information and Network Security Policy
IG09 Copyright and Copying Policy: Summary of National Guidance.
IG10 Subject Access Procedure
IG11 Media Policy and Procedure
IG12 Work Space Procedures
IG13 Buildings & Staff Relocation Guidance
IG14 Confidentiality in Communications Policy
IG15 Privacy Impact Assessment - Guidance
IG16 Privacy Impact Assessment
IG18 Privacy by Design Procedure

Appendix B - Other Relevant Legislation and Guidelines

Human Rights Act 2000

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

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

Regulation of Investigatory Powers Act 2000

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

Crime and Disorder Act 1998

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

The Act allows disclosure of person identifiable information to the Police, Local Authorities, Probation Service or the Health Service but only if the purposes are defined within the Crime and Disorder Act. The Act does not impose a legal requirement to disclose/exchange person identifiable information and responsibility for disclosure rests with the organisation holding the information. There should be a Crime and Disorder Protocol governing the disclosure/exchange and use of personal information within a local authority boundary agreed and signed by all involved agencies and organisations.

The Computer Misuse Act 1990

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

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

The Access to Health Records 1990

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

Access to Medical Reports Act 1988
This Act allows those who have had a medical report produced for the purposes of employment and/or insurance to obtain a copy of the content of the report prior to it being disclosed to any potential employer and/or prospective insurance company.

Legislation to restrict disclosure of personal identifiable information
- Human Fertilisation and Embryology (Disclosure of Information) Act 1992
- NHS (Venereal Diseases) Regulations of 1974 and 1992
- AIDS (control) Act 1987
- NHS Data Controllers and Primary Care Data Controller (Sexually Transmitted Diseases) Directions 2000
- Abortion Act 1967
- The Adoption Act 1976
- NHS Act 1977

Legislation requiring disclosure of personal identifiable information
- Public Health (Control of Diseases) Act 1984 & Public Health (Infectious Diseases) Regulations 1985
- Education Act 1944 (for immunisations and vaccinations to NHS Data Controllers from schools)
- Births and Deaths Act 1984
- Police and Criminal Evidence Act 1984

Appendix C - Definitions

Data Subject
A 'Data Subject' is a living natural person.

Personal Data
'Personal data' means any information relating to an identified or identifiable data subject.

Processing
'Processing' means any operation(s) performed on personal data, whether automated or not, such as collection, storage, organisation, adaption, alteration, use, disclosure, erasure or destruction.

Profiling
'Profiling' means any form of automated processing of personal data to evaluate certain personal aspects of the data subject. In particular to analyse or predict a data subjects performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements.

Controller
'Controller' or 'data controller' means a natural or legal person, public authority, agency or body which alone or jointly determines the purpose and means of processing personal data.

Processor
'Processor' or 'data processor' means a natural or legal person, public authority, agency or body that processes personal data on behalf of a controller.

Third Party
'Third party' means any natural or legal person, public authority, agency or body other than:

- the data subject,
- controller,
- processor and
- persons who are under the direct authority of the controller or processor who are authorised to process personal data.

Consent
'Consent' means any freely given, specific, informed and unambiguous indication of the data subject's wishes, by a statement or by clear affirmative action, signifies agreement to the processing of their personal data.

Data Concerning Health
'Data concerning health' means personal data relating to the physical or mental health of a data subject, including the provision of health care services, which reveal information about their health status.