# Data Protection Policy

## 1. Introduction

**1.1.** This policy describes the approach, procedures, and duties of the Scottish Hospitals Inquiry (hereinafter referred to as "the Inquiry") regarding the appropriate handling of the data of all natural persons.

**1.2.** This policy also fulfils the Inquiry's obligation to have in place an appropriate policy document under and in terms of the Data Protection Act 2018.

**1.3.** The Inquiry is committed to ensuring compliance with all applicable data protection legislation. The Inquiry's staff members, its Data Processors, any Joint Data Controllers, and any Data Controllers the Inquiry shares Personal Data with are responsible for adhering to the terms of this policy.

**1.4.** The Inquiry aims to adhere to the principles listed in the Appendix to this policy. This policy and the Inquiry's procedures set out how the Inquiry complies with those principles.

**1.5.** The Inquiry is registered as a Data Controller with the Information Commissioner's Office (registration number ZA775906). As a registered Data Controller, the Inquiry is obligated to collect, process, and store data in accordance with all applicable legislation, including:

**1.5.1.** The United Kingdom General Data Protection Regulation[1] ("the GDPR")
**1.5.2.** The Data Protection Act 2018 ("the 2018 Act")
**1.5.3.** The Data Protection, Privacy and Electronic Communications (Amendments etc.) (EU Exit) Regulations 2019/419

**1.6.** In this Policy, the following definitions apply:

**1.6.1.** "**Data Controller**" means the organisation or natural person determining the means and purposes of processing Personal Data.
**1.6.2.** "**Data Processor**" means the any organisation or natural person who is processing Personal Data on behalf of a Data Controller.
**1.6.3.** "**Data Subject**" means the living natural person in relation to whom Personal Data is processed.
**1.6.4.** "**DPO**" means Data Protection Officer.
**1.6.5.** "**ICO**" means the Information Commissioner's Office.

[1] The General Data Protection Regulation (EU) 2016/679 as incorporated by section 3 of the European Union (Withdrawal) Act 2018

1.6.6. "**Joint Data Controller**" means the organisation processing Personal Data in conjunction with another Data Controller for a common purpose.

1.6.7. "**Personal Data**" means any data, whether electronic or in hard copy, which is capable of identifying, directly or indirectly, a living natural person.

1.6.8. "**Processing**" means collecting, recording, sharing, organising, structuring, storing, adapting, altering, retrieving, disclosing, using, handling, or making available in any other way.

1.6.9. "**QEUH**" means the Queen Elizabeth University Hospital in Glasgow.

1.6.10. "**RHCYP/DCN**" means the Royal Hospital for Children and Young People and Department of Clinical Neurosciences in Edinburgh.

1.6.11. "**Sensitive Personal Data**" means any Personal Data, whether electronic or in hard copy, which reveals: racial or ethnic origin; political opinions; religious or philosophical beliefs; trade union membership; genetic data; biometric data; health data; data concerning a person's sexual life; or data concerning a person's sexual orientation.

## 2. Personal Data

2.1. In the course of its work, the Inquiry will request, receive, and process Personal Data relating to a variety of Data Subjects. Data Subjects may include but will not be limited to: Inquiry staff; core participants; witnesses; members of the public; patients or former patients of the QEUH or RHCYP/DCN; families of those patients; members of staff or former members of staff of Greater Glasgow Health Board or Lothian Health Board; employees of core participants; and employees of any other organisation assisting the Inquiry.

2.2. The Personal Data processed by the Inquiry may include, but will not be limited to, Data Subjects': names; dates of birth; postal addresses; email addresses; other contact details; written or oral statements from witnesses and other parties; health records; personnel records; copy emails and communications; audio recordings; video footage; and more.

2.3. The Inquiry will obtain Personal Data through various routes from both individuals and organisations who are able to assist the Inquiry's investigations. These routes may include, but are not limited to:

2.3.1. The voluntary production of information to the Inquiry by core participants and by individuals or organisations who are assisting the Inquiry;

2.3.2. The production of information to the Inquiry in response to a request by the Inquiry pursuant to Rule 8 of the Inquiries (Scotland) Rules 2007;

2.3.3. The production of information to the Inquiry in response to a request by the Inquiry pursuant to section 21 of the Inquiries Act 2005;

2.3.4. The production of information to the Inquiry in response to a Call for Evidence published by the Chair;

2.3.5. Information obtained by the Inquiry when it is contacted by a Data Subject or when the Inquiry contacts a Data Subject;

2.3.6. Information obtained by the Inquiry orally by speaking to Data Subjects

[2] Remit & Terms of Reference | Hospitals Inquiry

(in person or via telephone or video call).

**2.3.7.** Information made available by witnesses or other parties at hearings;

**2.3.8.** Information gathered during the research and investigative process; and

**2.3.9.** If a Data Subject works with, or applies to work with, the Inquiry.

**2.4.** The Inquiry aims to process Personal Data fairly and in a transparent manner. The Inquiry may only lawfully process the Personal Data of Data Subjects if it can rely on one of the following grounds:

**2.4.1.** **Public task:** It is necessary for the Inquiry to process the Personal Data in question in order to perform a task in the public interest or in the exercise of official authority vested in the Inquiry.

**2.4.2.** **Legal obligation:** It is necessary for the Inquiry to process the Personal Data in question in order to fulfil a legal obligation.

**2.4.3.** **Contract:** It is necessary for the Inquiry to process the Personal Data in question in order to fulfil a contract, or anticipated contract, with the Data Subject.

**2.4.4.** **Consent**: the Data Subject has given the Inquiry their clear, informed, and freely given consent for their Personal Data to be processed for a specific purpose. Where the Inquiry is relying on this basis for processing, it will obtain and retain written consent from the Data Subject in a Consent Form. Data Subjects are entitled to withdraw their consent at any time.

**2.4.5.** **Vital interests:** It is necessary for the Inquiry to process the Personal Data in question in order to protect the life of the Data Subject or of another person.

**2.4.6.** **Legitimate interest:** It is necessary for the Inquiry to process the Personal Data in question for the purposes of a legitimate interest. This basis cannot be relied on where the interests are overridden by the interests or fundamental rights and freedoms of the Data Subject. This basis should only be relied on where no other basis applies.

**2.5.** When processing Personal Data, the Inquiry will rely on the public task and legal obligation grounds in the majority of cases. The processing of Personal Data is required to ensure the Inquiry, with statutory functions and powers under the Inquiries Act 2005 and Inquiries (Scotland) Rules 2007, has all the necessary information to operate and fulfil its Terms of Reference[2] which is a task and function in the public interest under and in terms of section 8(c) of the 2018 Act.

**2.6.** The Inquiry will also require to process Sensitive Personal Data. In order to process Sensitive Personal Data, the Inquiry must be able to rely on an **additional** basis for processing Sensitive Personal Data from one of the following grounds:

**2.6.1.** Reasons of substantial public interest;

**2.6.2.** Consent;

**2.6.3.** Public health;

**2.6.4.** Health or social care;

**2.6.5.** Archiving, research, and statistics;

[3] Remit & Terms of Reference | Hospitals Inquiry

**2.6.6.** Employment, social security, and social protection;
**2.6.7.** Vital interests;
**2.6.8.** Not-for-profit bodies;
**2.6.9.** Legal claims or judicial acts;
**2.6.10.** Publicity.

**2.7.** The Sensitive Personal Data processed by the Inquiry may include, but will not be limited to, Data Subjects': medical and health data of patients or former patients of the QEUH and/or the RHCYP/DCN; trade union membership of staff employed at, or in relation to, the QEUH and/or the RHCYP/DCN; genetic data; biometric data; and more.

**2.8.** When processing Sensitive Personal Data, it is likely the Inquiry will rely on the reasons of substantial public interest ground in the majority of cases. This ground may be relied on as the Inquiry has a statutory and governmental purpose pursuant to section 10(3) and paragraph 6 of Schedule 1 to the 2018 Act. The processing of Sensitive Personal Data is required to ensure the Inquiry, with statutory functions and powers under the Inquiries Act 2005 and Inquiries (Scotland) Rules 2007, has all the necessary information to fulfil its Terms of Reference[3] which is a task and function of substantial public interest.

**2.9.** The Inquiry will not process any Personal Data (including Sensitive Personal Data) for any other purpose other than the purpose for which it was collected.

**2.10.** Further information about how the Inquiry obtains Personal Data, and which lawful bases it relies on for processing, can be found in the Inquiry's Privacy Notice and its Protocol on the Receipt and Handling of Information and Evidence. The Inquiry should make available its Privacy Notice to every Data Subject whose Personal Data is processed by the Inquiry. The Inquiry has published its Privacy Notice on its website and same can be found at Privacy Notice | Hospitals Inquiry.

## 3. Data Sharing

**3.1.** The Inquiry will require to share Personal Data with third parties who are not part of the Inquiry team. The Inquiry will only share Personal Data with third parties when it has a legal basis to do so. Such third parties may include but will not be limited to: core participants (including their legal representatives); witnesses; experts who are assisting the Inquiry team; counsel; external consultants or service providers; press agencies; the Scottish Government; the Keeper of the Records of Scotland; and the wider public.

**3.2.** Any third parties that the Inquiry shares Personal Data with may also be Data Controllers or they may be Data Processors. Data Controllers will determine their own means and purposes of processing the Personal Data. Joint Data Controllers will determine the means and purposes of processing the Personal Data in conjunction with the Inquiry. Data Processors will process the Personal Data on behalf of the Inquiry (for example, HR service providers or sheriff officers).

[4] Remit & Terms of Reference | Hospitals Inquiry

**3.3.** When the Inquiry shares Personal Data with Data Processors, Joint Data Controllers, and Data Controllers it will require them to enter into a written agreement, where appropriate, requiring adherence with all applicable legislation. In any event, Data Processors, Joint Data Controllers, and Data Controllers that the Inquiry shares Personal Data with will be expected to process any such Personal Data lawfully and in accordance with all applicable legislation and this policy.

**3.4.** Due to its nature and duties as a statutory public inquiry under the Inquiries Act 2005, the Inquiry aims to be as transparent as possible. Part of the Inquiry's statutory role is to make public the information it has considered in reaching its final conclusions. The Inquiry will conduct a number of public hearings in the course of its investigations . Those hearings may refer to Personal Data in the oral or documentary evidence of witnesses and core participants. Hearings will be accessible by any member of the public and will be video and audio recorded for public viewing on the internet. The Inquiry will also make public, via its website, in the course of hearings, and possibly by other means, the evidence, witness statements, and hearing transcripts that are being referred to in the course of its investigations. Some of this information will constitute Personal Data (including Sensitive Personal Data). Should any Data Subject wish for their Personal Data to be redacted or restricted prior to publication, they should refer to the Inquiry's Protocols on Redaction and Restriction.

**3.5.** The Inquiry will publish a final report and all of the Inquiry's key documents and information (including the contents of its website) that informed the report will be sent to the Keeper of the Records of Scotland for preservation in line with provisions under the Inquiries Act 2005 and the Inquiries (Scotland) Rules 2007. Such report and records may contain Personal Data and will be accessible by the general public.

**3.6.** Where it is necessary for any Personal Data to be transferred outside of the UK (for example, due to the location of a service-provider's systems), the Inquiry will ensure that it complies with all applicable legislation.

## 4. Data Security

**4.1.** The Inquiry aims to ensure the secure storage and handling of Personal Data whether in hard copy or in electronic format. Personal Data (in whichever format including documents and electronic storage devices) must be stored securely in a place where individuals other than the Inquiry staff and those permitted by the Inquiry cannot access it.

**4.2.** Inquiry staff are trained regarding their data protection obligations and duties and are expected to familiarise themselves with the content of this Policy and the following requirements:

**4.2.1.** Staff must ensure a clear desk when not occupied, whether in the Inquiry's offices or at a remote location.

**4.2.2.** Staff must securely lock their computer or laptop when leaving same unattended at all times.

**4.2.3.** Staff must not leave hard copy documents or moveable hard copy storage devices (such as a USB) unattended at any time.
**4.2.4.** Staff must not view Personal Data when using public transport without an appropriate privacy screen.
**4.2.5.** Where transporting Personal Data (whether hard copy or in electronic format on a device), staff must carry same in a lockable bag or briefcase.
**4.2.6.** Where processing Personal Data via telephone, staff must ensure that they cannot be observed or overheard.
**4.2.7.** Staff are permitted to use only their allocated secure Inquiry email account when processing Personal Data.
**4.2.8.** Staff are supplied with secure double-encrypted password controlled laptops. Staff may also be supplied with a secure double-encrypted password controlled mobile telephone.
**4.2.9.** Staff are not permitted to share their passwords with any other individual or colleague.
**4.2.10.** Staff must only use approved portable storage devices issued by the Inquiry which are password-protected and AES256 self-encrypting and are compliant with the ICO's guidelines.

**4.3.** The Inquiry will undertake official business by remote video conferencing only via approved software solutions which utilises end-to-end encryption using official Inquiry accounts and devices. Approved solutions are:

**4.3.1.** Microsoft Teams (video/audio)
**4.3.2.** Skype/Skype for Business (video/audio)
**4.3.3.** WebEx (video/audio)
**4.3.4.** WhatsApp (video/audio)
**4.3.5.** Mobile/Mitel Telephone (audio only)
**4.3.6.** PGI (audio only)

**4.4.** Any hard copy documents or material containing Personal Data held by the Inquiry will be stored securely in lockable cabinets.

## 5. Data Protection Officer

**5.1.** The Inquiry has appointed a Data Protection Officer (DPO). A DPO is responsible for ensuring the Inquiry's compliance and implementation of all applicable data protection legislation. The DPO will also liaise with the ICO, act as a point of contact for all Personal Data matters, and carry out regular risk assessments and audits.

**5.2.** The Inquiry's DPO is Ann Kerr who can be contacted at ann.kerr@hospitalsinquiry.scot.

**5.3.** The Inquiry's DPO has carried out a Privacy Impact Assessment. The Inquiry's DPO also maintains a record of its processing activities. Should any individual have any questions about the Inquiry's Privacy Impact Assessment, or require further information in relation to same, they may contact the Inquiry's DPO at ann.kerr@hospitalsinquiry.scot.

# 6. Data Subject Rights

**6.1.** Data Subjects have rights in law in respect of their own Personal Data processed by the Inquiry. The Inquiry is obligated to respond to any Data Subject who seeks to exercise those rights. All Data Subject rights will be processed by the Inquiry's DPO. Should a Data Subject wish to exercise any of their Personal Data rights, they may email the Inquiry's DPO at ann.kerr@hospitalsinquiry.scot. The Inquiry will require copy valid photographic identification, for example, a passport or driving licence, prior to fulfilling a Data Subject request. Any requests made otherwise in writing or verbally to any member of the Inquiry's staff will be passed to, and processed by, the Inquiry's DPO. The Inquiry's DPO will maintain a register of all requests by Data Subjects to exercise any rights and the Inquiry's response to same.

**6.2.** The rights of Data Subjects are not absolute and may be subject to certain exemptions and/or conditions. Each request will be considered and determined on its own merits. The Inquiry will only refuse a request where it has a legal basis to do so and will provide its reasons for refusal to the Data Subject.

**6.3.** The Inquiry will respond to Data Subjects no later than one calendar month from the date of receipt of the request. In certain circumstances, the Inquiry may seek to extend the timescale for responding and, where it does so, it will inform the Data Subject no later than one calendar month from the data of receipt of the request. The Inquiry will not charge a fee for complying with any of the following requests unless it is supplying further copies of data already provided to the Data Subject or unless the request is manifestly unfounded or excessive.

**6.3.1.** **The right to be informed:** Data Subjects have the right to know what Personal Data is held about them and why. The Inquiry fulfils this requirement by supplying a Privacy Notice to every Data Subject who is in contact with the Inquiry and by making same available on its website[4]. The Inquiry must supply its Privacy Notice to Data Subjects at the point it collects their Personal Data where possible. Where the Inquiry obtains Personal Data from third parties, it will supply a Privacy Notice to the Data Subjects (where possible) within one month. The Inquiry will review its Privacy Notice, and update it where necessary, every six months.

**6.3.2.** **The right of access:** Data Subjects have the right to access, or obtain a copy of any Personal Data held about them. Where a third party makes a request to access Personal Data on behalf of a Data Subject, the Inquiry will require to be satisfied that the third party has been authorised to act on behalf of the Data Subject. If further information is required before processing the request, the timescale for responding will be paused until the further information is received.

**6.3.3.** **The right to rectification:** Data Subjects have a right to request that their Personal Data be corrected should it be inaccurate or incomplete. Such a request should be accompanied by supporting evidence if appropriate. If the Inquiry is satisfied that the Personal Data is accurate, it may refuse the request and will supply the reasons for doing so.

4 Privacy Notice | Hospitals Inquiry

6.3.4. **The right to erasure:** Data Subjects have a right to request that their Personal Data be deleted by the Inquiry. The Inquiry may only be required to delete the Personal Data if it is no longer necessary for the purpose it was originally collected for. The right to erasure does not apply where processing is necessary for the performance of a task in the public interest or in the exercise of official authority.

6.3.5. **The right to restrict processing:** Data Subjects have the right to request that the processing of their Personal Data by the Inquiry be restricted. Data Subjects also have the right to object to the processing of their Personal Data. This means the Data Subject wishes to limit the way the Inquiry uses their Personal Data for a particular reason. If a request to restrict is accepted by the Inquiry, it will make the Personal Data unavailable for use by the Inquiry team.

6.3.6. **The right to data portability:** Data Subjects have the right to request from the Inquiry the Personal Data they have supplied in a structured, commonly used, and machine readable format. Data Subjects also have the right to request that the Inquiry transfers their Personal Data directly to another Data Controller. This right only applies where the Inquiry is relying on the Data Subject's consent or on the performance of a contract for processing.

6.3.7. **The right to object**: Data Subjects have the right to object to the Inquiry processing their Personal Data. This may be in relation to all or some of the Personal Data being processed. Data Subjects should explain why they object to their Personal Data being processed. Upon a successful objection, the Inquiry may stop processing the Personal Data. The Inquiry will continue to process the Personal Data if it has compelling legitimate grounds which override the interests of the Data Subject, or if processing is in relation to a legal claim.

6.3.8. **Rights related to automated decision making including profiling**: Profiling means the automated processing of Personal Data to evaluate certain things about a Data Subject. Automated decision making means making a decision solely by automated means without any human involvement. The Inquiry will ensure that it complies with the requirements of the UK GDPR and other applicable data protection legislation should it process Personal Data in this manner.

# 7. Personal Data Breaches

7.1. A Personal Data Breach occurs when there is an accidental or unlawful unauthorised disclosure, access, destruction, loss, alteration of Personal Data. Examples of Personal Data Breaches include, but are not limited to:

7.1.1. Sending an email containing Personal Data to the wrong recipient.
7.1.2. Failing to redact Personal Data where it should have been.
7.1.3. Misplacing or losing hard copy Personal Data.

**7.2.** Any member of staff working with the Inquiry, any individual or body acting as Data Processor for the Inquiry, and any individual or body acting as a Joint Data Controller or Data Controller with the Inquiry can be responsible for a data breach.

**7.3.** Where a Personal Data Breach, suspected or otherwise, occurs by any member of the Inquiry's staff, any individual or body acting as Data Processor for the Inquiry, or any individual or body acting as a Joint Controller or Data Controller with the Inquiry, the Inquiry's DPO will be informed immediately upon becoming aware of the breach. The Inquiry's DPO will be informed of:

**7.3.1.** The nature of the Personal Data Breach;
**7.3.2.** How the Personal Data Breach occurred; and
**7.3.3.** The impact of the Personal Data Breach on Data Subjects.

**7.4.** Steps should be taken by the individual responsible for the Personal Data Breach to mitigate risks where possible. An example of mitigation may be requesting that an email sent to an unintended recipient is deleted and purged.

**7.5.** The Inquiry's DPO will log the Personal Data Breach internally in every case and maintain a register of Personal Data Breaches made by or on behalf of the Inquiry. The register will record the nature of the breach, the date and time it occurred (or the date and time the Inquiry became aware of it), the consequences of the breach, measures taken to mitigate the breach, and whether the breach is reportable to the ICO. The Inquiry's DPO will also record his reasons for reporting, or not reporting, any Personal Data Breaches to the ICO and affected Data Subjects.

**7.6.** Should the Inquiry's DPO consider that the Personal Data Breach will likely result in a risk to the rights and freedoms of affected Data Subjects, he will inform the ICO within 72 hours of the breach occurring, or within 72 hours of the Inquiry becoming aware of the breach.

**7.7.** Should the Inquiry's DPO consider that the Personal Data Breach will likely result in a high risk to the rights and freedoms of the Data Subjects involved, he will inform those Data Subjects of the breach without undue delay. Data Subjects affected by a Personal Data Breach will be informed of: the nature of the breach; a point of contact for more information, most likely the Inquiry's DPO; the likely consequences of the Personal Data Breach; and any measures taken by the Inquiry to deal with the Personal Data Breach.

**7.8.** The Inquiry's DPO will also inform any relevant third parties of a Personal Data Breach in accordance with any written agreements that the Inquiry is party to.

## 8. Retention and Destruction

**8.1.** Due to the nature of the Inquiry, Personal Data (including Sensitive Personal Data) relevant to the Inquiry's Terms of Reference will be retained by the Inquiry until the Inquiry concludes and its final report is published. Personal Data (including Sensitive Personal Data) collected may require to be referred to in the Inquiry's later stages in order to fulfil its task of addressing its Terms of Reference and its statutory duty to compile a report. Due to the nature and limited lifespan of a public inquiry, it is

unknown when the Inquiry will conclude and publish its final report. Therefore, all relevant Personal Data and Sensitive Personal Data collected will be retained by the Inquiry for the duration of the Inquiry's limited lifespan.

**8.2.** At its conclusion, all relevant Personal Data and Sensitive Personal Data that the Inquiry has processed in carrying out its functions, reaching its conclusions, and forming its report will be passed to, and retained by, the Keeper of the Records of Scotland and will be available to the wider public. This is a statutory function and duty of a public inquiry under and in terms of the Inquiries (Scotland) Rules 2007.

## 9. Complaints

**9.1.** Should there any be concerns, queries, or complaints regarding the Inquiry's processing of Personal Data, the Inquiry's DPO, Ann Kerr, should be contacted in the first instance at ann.kerr@hospitalsinquiry.scot.

**9.2.** Should any party remain unsatisfied with the Inquiry's processing of Personal Data, they may contact the ICO in Scotland office at:

**9.2.1.** The Information Commissioner's Office – Scotland
Queen Elizabeth House
Sibbald Walk
Edinburgh
EH8 8FT
**9.2.2.** 0303 123 1115
**9.2.3.** Scotland@ICO.org.uk

## 10. Version control

**10.1.** This version of the Data Protection Policy is dated 19 March 2021 and is issued under the authority of the Chair of the Scottish Hospitals Inquiry. It is the first version of this Policy which will be reviewed every 6 months.

## 11. Appendix

**11.1.** The UK GDPR principles for processing require that Personal Data shall be:

"(a processed lawfully, fairly and in a transparent manner in relation to individuals ('**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 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 subject to implementation of the appropriate technical and organisational measures required by the GDPR in order to safeguard the rights and freedoms of individuals ('**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'**)."

**11.2.** The Inquiry shall be responsible for, and be able to demonstrate compliance with, paragraph 11.1 ('**accountability'**).