Data Protection Policy

NHS Property Services

Document Name, Version Number & Approval Date	Title: Data Protection Policy Version Number:2.1 Approval Date: 27 February 2023

Policy Owner	Department: Information Governance

Supporting Procedures & Additional Information	Data Protection Act 2018 General Data Protection Regulation Information Governance Policy Data Breach Policy Data Protection Impact Assessment Policy Data subject rights policy Access to CCTV Policy Corporate Records Management Policy Acceptable Use Policy Whistleblowing Policy Code of Conduct or other HR related policies/procedures www.ico.org.uk

NOTE: This policy should be reviewed annually and may be amended or replaced at any time.

DOCUMENT HISTORY

Version	Issue Date	Author(s)	Summary of Changes
V1.0	28 March 2019	Information Governance Officer	
V2.0	May 2021	Head of Information Governance	Refresh content following review by DP consultant.
V2.1	February 2023	Information Governance Lead	Function name change updated from TS to D&D

CONTENTS

1. PURPOSE

1.1. NHS Property Services (NHSPS) has a duty to protect and safeguard personal data. Operating in clear and transparent ways, we put data protection and privacy at the heart of our organisation. Processes are created and developed with Privacy by Design and by Default to ensure that the personal data we hold is processed in the safest way.

1.2. This policy provides an overview of our legal obligations and corporate expectations to data processing and handling. This policy will primarily focus on the:

- Data Protection Act 2018
- General Data Protection Regulation (GDPR).

1.3. Failure to comply with this policy or data protection legislation may result in serious repercussions for both the organisation and the individual concerned.

1.4. Organisations may face significant fines of up to 4% of global turnover or £17,500,000 (whichever is higher).

1.5. Individuals may face penalties such as criminal proceedings in cases of negligence, fraud or deliberate misuse.

1.6. For further information on data protection or information related legislation, please contact the Information Governance team by emailing dpo@property.nhs.uk.

2. SCOPE

2.1. This framework applies to all colleagues within NHSPS, including agency staff, independent contractors, honorary contracts, volunteers, trainees, and students on work experience placements.

3. RESPONSIBILITIES

All colleagues

3.1. Anyone working for or on behalf of NHSPS has a legal responsibility to protect personal data and process data in accordance with the data protection principles. This includes operating in a lawful, fair and transparent manner.

3.2. NHSPS expects everyone to operate in accordance with this policy and within the scope of their role. Any additional processing which occurs outside of your role must be agreed and authorised by the appropriate line manager or director.

3.3. If a request by or on behalf of an individual for information held about them or any other data subject's rights in relation to their personal data is received, you must immediately notify their line manager and the DPO and follow the Procedure for managing personal data requests.

3.4. If you work from home, data must be handled in accordance with the Acceptable Use Policy. Particular attention should also be given to ensure personal data is safeguarded at home.

3.5. You must complete mandatory GDPR training annually.

3.6. You should understand that breaches of this Policy may result in disciplinary action, up to and including dismissal.

All managers

3.7. All managers are responsible for the promotion of the GDPR as outlined within this policy and associated policies within their teams.

DPO

3.8. NHSPS is required to appoint a Data Protection Officer by the GDPR.

3.9. The DPO has the responsibility:

- to inform and advise us of our data protection processing obligations.
- to monitor our data protection compliance.
- to monitor our data protection policies.
- to assign data protection responsibilities.
- to raise data protection awareness.
- to ensure colleagues are trained in data protection.
- to audit or facilitate an audit of the organisation.
- to provide advice on and monitor Data Protection Impact Assessments.
- to liaise and cooperate with the Information Commissioner's Office (ICO).
- to act as a single point of contact for the ICO.

Senior Information Risk Officer

3.10. The SIRO has overall responsibility for leading and fostering a culture that values, protects and uses information for the success of the organisation and benefit of its customers.

Caldicott Guardian

3.11. The Chief Operating Officer has been appointed Caldicott Guardian. Whilst NHSPS does not process patient identifiable information, they will:

- Ensure NHSPS satisfies the highest practical standards for handling patient identifiable information (in the case that this occurs).
- Oversee any arrangements, protocols and procedures where confidential patient information may be shared with external bodies both within, and outside, the NHS.

Information Governance Team

3.12. The Information Governance Team is responsible for:

- the operational oversight of all data protection and confidentiality issues.
- the provision of systems and facilities to support accurate, legally compliant, secure and efficient information governance.
- for the day-to-day oversight of data protection issues and for ensuring that data is handled in accordance with NHS PS policy and legal requirements.
- dealing with Subject Access Requests under the GDPR and for ensuring sufficient fair processing information is available to users of NHSPS services.

4. GDPR Definitions

4.1. This section provides an overview of the core definitions of data protection and data processing.

Anonymisation

4.2. Where identifiers have been removed so a data subject cannot be identified by anyone. Further information on anonymisation can be obtained from the Information Commissioner's website.

Consent

4.3. Agreement which must be freely given, specific, informed and be an unambiguous indication of the Data Subject's wishes by which they, by a statement or by a clear positive action, signify agreement to the Processing of Personal Data relating to them.

Data subject

4.4. A living individual or natural person.

Data controller

4.5. An organisation who decides how data is used (processed). The GDPR defines this as 'the natural or legal person, public authority, agency, or other body which, alone or jointly with others, determines the purposes and means of processing of personal data; where the purposes and means of such processing are determined by Union or Member State law, the controller or the specific criteria for its nomination may be provided by Union or Member State law' (Article 4(7)).

Data processor

4.6. An organisation or person who processes data on a data controller's behalf. The GDPR defines this as 'a natural or legal person, public authority, agency, or other body which processes personal data on behalf of a controller' (Article 4(8)).

Data protection legislation

4.7. Laws which organisations must follow to protect and safely process personal data. These laws are made by the UK government and the European Parliament.

DPA 2018

4.8. Data Protection Act 2018 (UK law).

GDPR

4.9. General Data Protection Regulation – Regulation (EU) 2016/679 (EU law).

Identifier

4.10. Something which allows a data subject to be identified. This includes anything such as a name, address or eye colour. An identifier could be anything if someone can tell, directly or indirectly, who is being described.

Personal data

4.11. The GDPR defines personal data as 'any information relating to an identified or identifiable natural person. An identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person' (Article 4(1)). This can include:

- tenants
- service users
- contractors
- employees
- and other customers.

Personal Data Breach

4.12. Any act or omission that compromises the security, confidentiality, integrity or availability of Personal Data or the physical, technical, administrative or organisational safeguards that we or our third-party service providers put in place to protect it. The loss, or unauthorised access, disclosure or acquisition, of Personal Data is a Personal Data Breach.

Privacy Notices

4.13. Separate notices setting out information that may be provided to Data Subjects when the Company collects information about them. These notices may take the form of general privacy statements applicable to a specific group of individuals (for example, employee privacy notices or the website privacy policy) or they may be stand-alone, one-time privacy statements covering Processing related to a specific purpose.

Privacy by Design

4.14. Implementing appropriate technical and organisational measures in an effective manner to ensure compliance with the UK GDPR.

Processed or processing

4.15. Any activity that involves the use of Personal Data. It includes obtaining, recording or holding the data, or carrying out any operation or set of operations on the data including organising, amending, retrieving, using, disclosing, erasing or destroying it. Processing also includes transmitting or transferring Personal Data to third parties.

Pseudonymisation

4.16. Where an identifier has been changed so only those who know how it has been changed can identify the data subject. The GDPR defines this as 'the processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is kept separately and is subject to technical and organisational measures to ensure that the personal data are not attributed to an identified or identifiable natural person' (Article 4(5)).

Special category data

4.17. Special category data includes:

- Race or ethnic origin
- Political opinions
- Religious or philosophical beliefs
- Trade union membership
- Genetic data
- Biometric data
- Health data
- Sexual history and/or sexual orientation
- Criminal data

5. Data Protection Principles

5.1. NHS Property Services processes personal data in accordance with the six GDPR principles.

5.2. These principles act as a single framework for all processing activities which involve personal data about living individuals. The GDPR states that personal data shall be:

A. Processed lawfully, fairly and in a transparent manner.

5.3. NHSPS have a legal basis of processing. Article 6 of the GDPR provides six legal basis's which allows us to **process personal data**. We must meet only one of these conditions and it is up to us to determine which is the most appropriate reason for each process. Data protection legislation allows us to process personal data if:

1. The data subject has given their consent.

2. The processing is necessary for the performance of a contract to which the data subject is party, or for the taking of steps at the request of the data subject with a view to entering a contract.

3. The processing is necessary for compliance with a legal obligation to which the data controller is subject to. This does not include contractual obligations.

4. The processing is necessary to protect the vital interests of the data subject or another person.

5. The processing is necessary of a task carried out in the public interest or in the exercise of official authority vested in the controller.

6. The processing is necessary for the purpose of the legitimate interests of the controller or by a third party, except where such interests are overridden by the interests of fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child.

Special Category Data

5.4. Some categories of personal data require a higher level of protection and care when processing. This data is known as special category data. If we are processing any special categories of personal data, we are required to have a second lawful reason to process. We are required to select an article 9 reason in addition to selecting an article 6 reason.

5.5. Article 9 of the GDPR allows us to process special category data if:

1. The data subject has provided explicit consent.

2. 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.

3. The processing is necessary to protect the vital interests of the individual subject or another natural person where the data subject is physically or legally incapable of giving consent.

4. The processing relates to information which has been made manifestly public by the data subject.

5. The processing is necessary for the establishment, exercise or defence of legal claims or whenever courts are acting in their judicial capacity.

6. The processing is necessary for the purposes of substantial public interest, proportionate and with due regard to the data subject's rights and freedoms.

7. Processing is necessary for health and social care purposes, including the assessment of the working capacity of the employee.

8. Processing is necessary for the purposes of public health.

5.6. Processing of personal data which falls outside of an individual's role may be deemed as unlawful. Unlawful purposes include, but are not limited to:

- unauthorised access to systems
- unauthorised sharing of data to third parties
- unauthorised downloading of personal data
- misuse or malicious use of data
- unauthorised deleting of data.

5.7. Processing personal data by any individual without a lawful and authorised purpose will be considered a breach of data protection legislation and may lead to the DPO reporting the individual to the Information Commissioner's Office.

B. obtained and used only for one or more specified and lawful purpose(s). Personal data should not be used for other purposes.

5.8. NHSPS must only collect data for specified, explicit and legitimate purposes and not further process in any manner incompatible with those purposes.

5.9. NHSPS has set out why we process personal data in our Privacy Notice which is set out on NHS Property Service's website at https://www.property.nhs.uk/privacy-policy/

5.10. To comply with this principle, NHSPS must maintain a record of how it uses personal data and ensure this is reflected in its Privacy Notice. If a new use of personal data is proposed that is not already covered by this, steps must be taken to ensure appropriate notice is given.

C. Adequate, relevant and limited to the specified purpose (data minimisation).

5.11. NHSPS has put in place several measures to achieve this, including:

1. Limiting access within our systems to stop data being used for irrelevant purposes.

2. Developing data retention policies which help us to ensure that unnecessary data is not kept.

3. Designing our processes, forms, and systems so as not to capture extraneous data.

5.12. It is the responsibility of all employees to ensure that personal data processing is adequate and limited to what is proportionate.

D. Accurate and, where necessary, up to date; and inaccurate personal data are erased and rectified without delay.

5.13. Where employees obtain information either directly from the data subject or via a third party, they must ensure the accuracy of the data held. We ordinarily test new systems before rolling them out more widely in order to establish that they maintain data accuracy.

5.14. If the data subject informs NHSPs of a (factual) inaccuracy, the data must be amended to reflect this.

E. Kept only for the amount of time required to fulfil the purpose (storage limitation)

5.15. NHSPS should not retain information for longer than is required to fulfil the purposes for which it is collected, as per the Records Management and Retention Policy.

F. Processed with integrity and confidentiality (appropriate security).

5.16. NHSPS will maintain technical and organisational measures to prevent or manage foreseeable incidents and identified risks which may affect the secure processing of personal data. All employees will be kept aware of security issues associated with the processing of data, through training and other measures.

5.17. Data protection and confidentiality clauses must be formally defined and included within third party contracts, and appropriate due diligence as to their security arrangements is performed.

5.18. When considering appropriate security NHSPS must consider whether the following steps are appropriate:

- Pseudonymisation ' a technique that replaces or removes information in a data set that identifies an individual and encryption.
- The ability to secure the confidentiality of data and the stability of the storage platforms ensuring business continuity access to data in the evident of physical or technical incidents.
- Regular testing and evaluating the effectiveness of security measures.

5.19. If there is a data security breach, data controllers are ordinarily required to report the breach to the Information Commissioner within 72 hours, unless the breach is unlikely to result in risk to the rights and freedoms of the data subject. Any incidents which might meet the threshold for reporting must be reported to the DPO.

5.20. It is therefore important any suspected data security breach is reported to the DPO as soon as possible. The DPO will then assess whether the breach is reportable to the ICO.

5.21. If a data breach is likely to create a high risk to the risks and freedoms of the data subject, there is an obligation to notify the affected data subjects directly. Again, the assessment of whether this is required will be undertaken by the DPO.

5.22. See the Data Breach Policy for further information.

6. Data Subject Rights

6.1. Under data protection legislation, twelve rights are available to data subjects:

- the right to be informed.
- the right to subject access.
- the right to rectification.
- the right to erasure.
- the right to restrict processing.

- the right to data portability.
- the right to object.
- rights in relation to automated decision making.
- the right to take judicial action against the ICO.
- the right to take judicial action against a controller or processor.
- the right to compensation.

6.2. Data protection principle four states that all personal data records must be accurate and, where possible, kept up to date. Article 16 of the GDPR gives the right for data subjects to rectify any errors to their personal data.

6.3. Data subjects can apply any of their rights by contacting the DPO.

6.4. Further information can be found in the Data Subject Rights Policy or by email on dpo@property.nhs.uk

7. SUBJECT ACCESS AND OTHER INFORMATION RIGHTS REQUESTS.

7.1. Individuals have a right under the GDPR to make a request in writing for a copy of the information held about them. This is called a subject access request. Subjects are also entitled to be given a description of the information, what it is used for, who it might be passed on to, and any other information held. Individuals have other rights under data protection law (for instance to ask for inaccurate data to be corrected or to object to our use of their data).

7.2. Any such request for information should be construed a subject access request unless part of the normal course of business. Such requests should be passed to the Data Protection Officer. Requests should ordinarily be dealt with within the legal timescale of one calendar month.

7.3. For further detail please see the policy on handling Subject Access Request or contact the Data Protection Officer.

8. COLLECTING AND USING PERSONAL DATA

8.1. When collecting personal data, we must ensure that we operate in accordance with the data protection principles.

8.2. All departments are responsible for:

- data quality and management
- management of processes and access to their systems
- Data Protection Impact Assessments.

Data quality and management

8.3. It is the responsibility of everyone to ensure that the data processed is correct at the point of collection. If you find any errors, these should be rectified as quickly as possible. If an individual is not authorised to make an amendment, these should be escalated to their manager for action.

8.4. You must also ensure that the data collected is appropriate to the purpose of processing. This includes ensuring that you have just enough data to carry out your process. You should not collect more data than is needed and should not keep personal data longer than required. Data should not be retained for a purpose of 'just in case'.

8.5. Departments must put in place adequate records management procedures which comply with corporate guidelines as issued by the Information Governance team. Further advice on retention, data quality and records management can be obtained from the Information Governance team.

Sending emails

8.6. Emails are the most common method of receiving communications from our customers, colleagues, and stakeholders. However, emails pose a significant risk to the organisation. When using emails, please be aware of the following:

- recipient inboxes may not be restricted to one user. Inboxes can be shared, and it is important to understand that any distribution of data to an inbox may not be viewed only by the intended recipient.
- Email addresses can auto complete when submitting them in the 'to', 'cc' or 'bcc' fields. Care should be taken to verify all entered email addresses prior to sending the email.
- Care must be taken when sending emails to pre-defined groups or distribution lists. Mailing lists may contain a larger audience than intended, including both internal and external recipients. When sending to a pre-defined group or distribution list, you should always check the intended recipients prior to clicking send.
- Work related emails, especially those containing personal data or special category data, must only be sent through NHSPS email addresses. Personal data must not be sent through accounts such as Gmail or Hotmail. This may be considered as a breach and investigated under the Data Breach Policy.
- Email inboxes must not be used as a storage or recording system. Emails constitute records, similar to that of a letter or fax. Emails must be uploaded to case management systems and deleted from inboxes. All records may only be retained for a fixed period of time. Keeping a record (including an email) longer than the retention period is considered to be a breach of the data protection principles.
- If you are required to provide proof that an email has been sent or received (non-repudiation), you should seek appropriate advice from the IT and Information Governance teams.

9. DATA STORAGE

9.1. All data must be stored in safe and secure locations to ensure data is processed in accordance with the law. Access to areas, both digital and physical, must be granted through locally agreed approval procedures.

9.2. Personal data held in physical locations must be:

- stored within NHS Property Services buildings
- locked with restricted access to specific individuals.

9.3. Most information should be available electronically, therefore taking physical files should only be done on an exceptions basis. If physical documents are taken home, you must ensure that:

- personal data is securely locked away and not left in vehicles,
- a record of when personal data has been taken outside of the office environment and when it has been returned,
- a record of who has taken personal data outside of the office environment.

9.4. Personal data held in digital locations must be:

- stored in NHS Property Services devices,
- restricted to particular users and teams,
- held on NHSPS servers where it is regularly backed up.

9.5. Access to screens or datasets which display other data subjects' data should not be given to anyone other than yourself or your team and mitigation, such as privacy screens, should be implemented.

9.6. Personal data must not be:

- transferred or stored on personal devices including, but not limited to:
  - mobile phones
  - MP3 or MP4 players
  - cameras
  - memory sticks (including USB sticks)
  - home computers or laptops
- emailed to an employee's home/personal email account/computer. Working from home should be through secure remote access or through work issued devices.
- stored on unencrypted devices.

10. SHARING PERSONAL DATA

10.1. Through the day-to-day operations of NHSPS, we are required to share personal data to ensure we can provide a service to our tenants, partners and stakeholders. Data protection legislation permits the sharing of data and considers sharing as a processing activity. When sharing personal data externally, NHSPS must ensure it meets its legal basis for processing in accordance with article six and article nine of the GDPR.

10.2. To ensure data is shared appropriately, all data sharing must also have one of the following:

- a law which requires data sharing
- a contract which specifies datasets to be shared

- an information sharing agreement/protocol which specifies datasets to be shared.
- the data subject's consent.

10.3. See the Data Sharing Policy for further information.

Information sharing agreements and protocols

10.4. Whilst best practice, an information sharing agreement or protocol is not a legal requirement. An agreement does not create a legal gateway if one does not already exist. However, we encourage agreements and protocols as they allow us to work with our partners to the same high standards.

10.5. All agreements and protocols, either led by NHS Property Services or a different data controller, must be reviewed by the Information Governance team. Agreements and protocols must not be signed by any officer, department or directorate without seeking advice and review from the Information Governance team or our Legal team.

10.6. Agreements and protocols should be drawn up following consultation between organisations. No agreement or protocol should be forced onto another organisation to sign, and all parties should work together to agree with the final wording.

Contracts

10.7. All contracts which involve the sharing of personal data must contain data protection and information governance clauses. Information supplied to processors and organisations working on our behalf can only be used for agreed purposes. Further use or disclosure for any other reason is not allowed without further consultation and the written consultation of the organisation.

10.8. Any further use may be subject to a full Data Protection Impact Assessment.

Internal Sharing

10.9. We do not require an information sharing agreement or protocol to share personal data internally. NHSPS is one data controller. However, information should not be shared freely between departments. When sharing data internally, information sharing must comply with the data protection principles.

10.10. All sharing must serve a purpose and be lawful. Internal data sharing proposals must be assessed in accordance with our Data Protection Impact Assessment Policy.

10.11. Non-sensitive personal data (data which does not fall under special categories of data) may be shared across the organisation and data processors working on our behalf to:

- maintain accurate records,
- recover costs owed to the organisation,
- streamline processes to achieve our legitimate purposes,
- preventing and detecting fraud.

10.12. We will make every effort to protect special category data and not share it between departments without the data subject's consent. However, special category data may be shared between our departments to protect the vital interests of the data subject.

11. DATA PROTECTION BY DESIGN & BY DEFAULT

11.1. We shall implement appropriate organisational and technical measures to uphold the principles outlined above. We will integrate necessary safeguards to any data processing to meet regulatory requirements and to protect individual's data rights. This implementation will consider the nature, scope, purpose and context of any processing and the risks to the rights and freedoms of individuals caused by the processing.

11.2. We shall uphold the principles of data protection by design and by default from the beginning of any data processing and during the planning and implementation of any new data process.

11.3. We ensure that, by default, personal data is only processed, when necessary for specific purposes and that individuals are therefore protected against privacy risks.

11.4. In all processing of personal data, we use the least amount of identifiable data necessary to complete the work it is required for and we only keep the information for as long as it is required for the purposes of processing or any other legal requirement to retain it.

11.5. Where possible, we will use pseudonymised data to protect the privacy and confidentiality of our colleagues and those we support.

12. DATA PROTECTION IMPACT ASSESSMENTS

12.1. All new systems used for data processing will have data protection built in from the beginning of the system change.

12.2. When NHSPS is considering a new project or service change initiative which will include the processing of personal data, consideration must be given by the project lead throughout the project development process to whether a Data Protection Impact Assessment (DPIA) needs to be completed.

12.3. DPIAs are a legal requirement for processing that is likely to be high risk. A DPIA will help identify and minimise data protection risks. Our DPIAs will take account of compliance risks, and also broader risks to individuals' rights and freedoms.

12.4. Not all new projects and ways of working require a full DPIA, however all project leads must submit a screening tool to verify eligibility. If a full DPIA is required, this must be carried out prior to the commencement of processing.

12.5. DPIAs must be carried out in accordance with the DPIA Policy. Please view this policy for further information or contact dpo@property.nhs.uk

12.6. Records of DPIAs shall be kept by the Information Governance Team.

13. CONFIDENTIALITY

13.1. At times, information may be accepted by the organisation in confidence or as part of a confidential relationship. Employees must not disclose confidential information to anyone else without the permission of the individual who first gave the information to them. However, in exceptional circumstances information can be shared without the individual's consent.

Redacting information

13.2. There may be situations where you need to redact personal or business sensitive information from documents you are sharing. Care should be taken when redacting information to ensure the redaction is a permanent one and cannot be removed by the recipient.

13.3. Data can also be disclosed in error can occur when data is not immediately visible on the screen but elsewhere within the file. For example, when setting up a template a user might have chosen to 'hide' certain data by setting the font colour to be the same as the background (e.g., white on white or black on black). Be sure to remove any data that should not be shared wider.

13.4. Contact the Information Governance Team for further details on redacting information.

13.5. We operate a Whistleblowing Policy, which provides information on what to do in these situations.

Leaving the organisation

13.6. Once an employee has left the organisation, all access to data must be restricted and access permissions to systems must be terminated.

13.7. This policy does not cover the remit of non-disclosure agreements. However, when an employee leaves the organisation, confidentiality must be adhered to and any further use of personal data is prohibited.

13.8. In cases where negligence is suspected, or an offence has occurred, the Data Protection Officer should be immediately informed. Further information on the process can be found in the Data Breach Policy.

TRAINING

13.9. The Data Protection Officer has responsibility for awareness-raising and training. The Information Governance team will review the training provided to ensure it remains relevant.

All-employee Mandatory Training

13.10. The following mandatory training modules are hosted on the learning Zone and must be completed by all colleagues annually:

- Data Protection.
- Confidentiality.

Focussed Training

13.11. Additional training can also be requested for teams or individuals requiring further information or to enable roles to be performed appropriately. Examples of training that could be provided are:

- CCTV training
- Responding to information requests to our suppliers and Trusts
- Dealing with Subject Access Requests.

14. MONITORING

14.1. Compliance with the policies and procedures in this document will be monitored via the Data Protection Officer and the Information Governance team, e.g., spot checks on CCTV compliance.

14.2. Independent reviews will also be performed by Internal Audit.

14.3. The Head of Information Governance is responsible for the monitoring, revision and updating of this document on a 2 yearly basis or sooner if the need arises.