MPS Care Group Privacy Notice

Data Protection

1. INTRODUCTION

1.1. MPS Care Group is committed to conducting its business in accordance with all applicable Data Protection laws and regulations (General Data Projection Regulation (GDPR) and Data Protection Bill (DPB) and in line with the highest standards of ethical conduct.

1.2. This policy sets out the behaviors of MPS colleagues and third parties in relation to the collection, use, retention, transfer, disclosure and destruction of any personal data belonging to an Identifiable Natural Person, the Data Subject.

1.3. Personal data is any information (including opinions and intentions) which relates to the Data subject. Personal data is subject to certain laws, which impose restrictions on how organization may process personal data. An organization that handles personal data and make decisions about its uses is known as a Data Controller. MPS Care, as a Data Controller, is responsible for ensuring compliance with the data protection requirements outlined in this policy Non-compliance may expose MPS Care to complaints, regulatory action, fines and/or reputational damage.

1.4. MPS Care CEO and management team is fully committed to ensuring continued and effective implementation of this policy and expect MPS Care Group colleagues and third parties to share in this commitment. Any breach of this policy will be taken seriously and may result in disciplinary action or business sanction.

1.5. The GDPR and DPB do not relate to records of the deceased. Access to health records of the deceased is governed by the 'Access to Health Records Act (1990)' which states:

(1) An application for access to a health record, or to any part of a health records, may be made to the holder of the record by any of the following,

(a) The patient; … (f) where the patient has died, the patient's personal representative and any person who may have a claim arising out of the patient's death.

2. SCOPE

2.1. This policy applies to MPS Care where a Data Subjects personal data is processed:

- By MPS Care colleagues (including whilst away from work)
- In the context of the business activities to MPS Care
- For the provision of goods or services to individuals (including those provided or offered free-of-charge) by MPS

- To actively monitor the behaviour of individuals.

2.2. This policy applies to all processing of personal data in electronic form including electronic mail and documents) or where it is held in manual files that are structured in a way that allows ready access to information about individuals.

2.3. This policy has been designed to establish a baseline for the processing and protection of personal data by MPS Care. Where national law imposes a requirement, which is stricter than imposed by this policy, MPS Care must follow the requirements in national law. Furthermore, where national law imposes a requirement that is not addressed in this policy, MPS Care must adhere to the relevant national law.

2.4. If there are conflicting requirements in this policy and national law, please contact MPS Care Data Protection Officer.

3. GOVERNANCE

3.1. Data Controller

MPS Care is the Data Controller for all personal data processed by MPS Care. MPS Care is responsible in making sure that it applies to the GDPR throughout the business and can provide compliance to the UKs Statutory Authority, the Information Commissioners Office (ICO).

MPS Care may enter into contracts with third parties, e.g. local authorities, CCGs, to provide a service on their behalf. This may lead to MPS Care determinant what information needs to be processed and determining the way that it is processed. Under these circumstances, the two parties will be joint Data Controllers. A contract is required to specify;

- The respective responsibilities of both parties
- The respective roles regarding the data subjects
- Who the data subject should contact in regards of each controller.

3.2. Data Processors

MPS Care may engage with the external bodies to carry out some processing on behalf of MPS Care.

All such processing will be governed by a contract to make sure that:

- The data is only processed for the purpose requested by MPS
- The data will not be shared with any other party
- The data processor is compliant to the GDPR
- MPS Cares data will be returned to MPS care when the contract ends and all copies held by the contractor will be destroyed.

3.3. Data Protection Officer

As required by GDPR, MPS Care has a Data Protection Officer. The DPO operates with independence and is granted all necessary authority. The DPO 's duties include:

a) Informing and advising MPS Care staff of the processing of data in accordance with Data Protection regulations and national law.
b) Ensuring Information Governance policies, including Privacy Notices, align with Data Protection regulations or national law
c) Providing guidance to carrying out Data Protection Impact Assessments (DPIAs)
d) Maintaining a record of personal data held by MPS Care and processing activities
e) Acting as a point of contact for and cooperating with the Information Commissioners Office (IC), the UKs Data Protection Authority
f) Informing and updating the ICO regarding MPS Care current and intended personal data processing activities as necessary
g) Establishment and operation of a system for logging and providing prompt and appropriate responses to the rights of data subjects.
h) Recording all incidents involving personal data and determining when the ICO/ and/or data subjects need to be informed of a breach.
i) Informing MPS Cares directors and managers of any potential corporate, civil and criminal penalties which may be levied against MPS and/or its colleagues for violation of applicable Data Protection laws.
j) Data Protection compliance monitoring
k) Ensuring the establishment of procedures and contractual provisions for obtaining compliance with this policy by any third party who: -
    - Provides personal data to MPS Care
    - Receives personal data from MPS Care
    - Has access to personal data collected or processed by MPS Care

3.4. Compliance Monitoring

The Data Protection Officer will carry out a Data Protection Compliance audit for all locations and departments to determine the level of compliance. Each audit will assess:

a. Compliance with Policy in relation to the protection of personal data, including
    - Raising awareness
    - Training of Colleagues
b. The effectiveness of Data Protection related operational practices, including:
    - Data subject rights (including involving the DPO)
    - Personal data transfers
    - Personal data incident management

- Personal data complaints handling
- The level of understanding of Data Protection policies and Privacy Notices
- The accuracy of personal data being stored
- The conformity of Data Processor activities
- The adequacy of procedures for redressing poor compliance of personal data breaches.

The DPO, in cooperation with key business stakeholders, will correct any identified deficiencies within a defined and reasonable timeframe, informing the management team.

3.5. Policy Dissemination and Enforcement

MPS Care Groups management team will ensure that MPS colleagues are aware of and comply with the contents of this policy.

In addition, MPS Care will ensure all third parties engaged to process personal data on their behalf are aware of and comply with the contents of this policy. Assurance of such compliance must be obtained from all third parties, in writing, prior to granting them access to personal data controlled by MPS Care.

3.6. Data Protection by Design

Data Protection by Design requires all risks involving personal data to be considered when:-

- New systems are being implemented
- Changes are being made to systems affecting the use of personal data
- Security or access criteria are being reviewed / changed
- Business processes involving personal data are changed.

Each of these projects or changes must go through an approval process before being implemented. The approval process is carried out by the Data Protection Impact Assessment (DPIA). All colleagues involved in any changes with systems, reports, processes or access must engage with the DPO and a DPIA will be carried out.

4 DATA PROTECTION PRINCIPLES|

MPS Care Group must apply the following GDPR principles to govern its collection, use, retention, transfer, disclosure and destruction of personal data:

Principle 1: Lawfulness, Fairness and Transparency

Personal data shall be processed lawfully, fairly and in a transparent manner in relation to the Data subject. MPS Care Group will inform the Data subject, through Privacy Notices (transparency) what data will be processed and how it will be processed (fairness), and the legal basis for the processing e.g. contract or opt-in (lawfulness)

Principle 2: Purpose Limitation
Personal data shall be collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes. MPS Care Group must specify wat the personal data collected will be used for and limit its use to the specified purpose.

Principle 3: Data Minimization
Personal data shall be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed. MPS Care Group must only store data that is necessary to carry out the task for which the data is being held.

Principle 4: Accuracy
Personal data shall be accurate and kept up to date. MPS Care Group must have in place procedures for identifying and addressing out-of-date, incorrect and redundant personal data.

Principle 5: Storage Limitation
Personal data shall be kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data is processed.

Principle 6: Integrity and Confidentiality (security)
Personal data shall be processed in a manner that ensures appropriate security of the personal data, including protection against unauthorized or unlawful processing and against accidental loss, destruction or damage. MPS Care Group must use appropriate technical and organizational measures to ensure the integrity and confidentiality of personal data is maintained.

Principle 7: Accountability
The Data Controller shall be responsible for and be able to demonstrate compliance. MPS Care Group must be able to demonstrate that the six Data Protection Principles are being applied through detailed policies, procedures, training and regular audits.

5 DATA COLLECTION

5.1. Data Sources

Personal data should only be collected from the data subject unless one of the following apply:-

a. The nature of the business purpose necessitates collection of the personal data from other persons or bodies, e.g. contract with Local Authority or CCGs.
b. The collection must be carried out under emergency circumstances in order to protect the vital interest of the data subject e.g. from a family member or General Practitioner
c. If personal data is collected from someone other than the data subject, the data subject must be informed of the collection unless one of the following apply:
   - The data subject has received the required information by other means

- The information must remain confidential due to the professional obligation
- A national law expressly provides for the collection, processing or transfer of personal data

Where is has been determined that notification to a data subject is required, notification must occur promptly, but in no case, later than:

- One calendar month from the first collection or recording of the personal data
- At the time of the first communication if used for communication with the data subject
- Prior to disclosure if it is to be disclosed to another recipient.

5.2 There are six legal bases for the processing of personal data:-

Data Subject Consent. Note that consent can be revoked.

a. MPS Care will obtain personal data only by lawful and fair means and where appropriate with the knowledge and consent of the individual concerned. Where a need exists to require and receive the consent of an individual prior to the collection, use of disclosure of their personal data, MPS is committed to seek such consent.

The DPO and management team will establish a system for obtaining and documenting data subject consent of the collection, processing and/or transfer of personal data. They system will include provisions for:-

- Determining what disclosures should be made to obtain valid consent
- Ensuring the request for consent is presented in a manner which is clearly distinguishable from any other matters and is made in an intelligible, easily accessible form and uses clear language
- Ensuring the consent is freely given and is not based on a contract that is conditional to the processing of personal data
- Documenting the date, method and content of the disclosure made, as well as the validity and scope of the consent given
- Providing a simple method for a data subject to withdraw their consent at any time.

Upon obtaining consent to the processing of personal data and data is collected, all appropriate disclosures will be made unless one of the following apply-

- The data subject already has the information
- The legal exemption applies to the requirements for disclosure and/or consent.

The disclosures may be given electronically or in writing.

2. It is necessary for the performance of a contract e.g. employment
All contracts created by MPS Care Group must ensure that the six principles are being adheres to:

- Privacy Notice covers the contract
- Collected personal data will only be used to fulfil the contract
- Only data necessary for the contract will be requested
- There is a means for ensuring that the data is correct
- MPS's Retention Schedule details the retention period
- The data will be kept secure and only accessed on a need to know basis.

Compliance with a legal obligation e.g. disclosing salary information to the HMRC
MPS Care Group will comply with all legal and statutory requirements with details included in the relevant Privacy Notices.

Protection of the vital interest of the data subject e.g. providing medical information in a life-threatening situation.

In the case of an emergency, MPS Care may engage with family members, medical professionals in order to protect the life of the data subject. Where residents have a 'Do not resuscitate order' on file, this will take precedence.

Carrying out a task in the public interest e.g. using CCTV for crime prevention
MPS Care may carry out tasked for Public Interest. These will typically be the use of CCTV for crime prevention and the tracking of IP addresses to ensure that no illegal activity is carried out by individuals using IT services offered by MPS Care e.g. business or free internet access.

Legitimate interest of MPS Care e.g. using photographs taken at a public event.
MPS Care Group may use the legal basis of 'legitimate interest' in order to process personal data or to process personal data for a purpose different to the original intention. For example MPS care may take photos or video footage at events which will capture individuals and the use of these will be for legitimate business interest of MPS and are not expected to significantly affect the rights and freedom of those caught on film.

5.3. Privacy Notices
MPS Care Group will make available Privacy Notices covering the processing of personal data for the following: -

- Staff (contractors, employees and volunteers)
- Care home residents
- Supporters (including fundraisers)

Privacy Notices should be provided at the point that the data subject provides their data.

6. DATA USE

6.1. Data Processing

MPS Care uses personal data for the following purposes:

- The administration of MPSs responsibilities as an employer
- The general running and business administration of MPS Care Group
- To provide services to MPS Care Group service users
- The ongoing administration and management of customer services
- MPS Care supporter activities.

The use of personal information should always be considered from the data subjects perspective and whether the use will be within his/her expectations or if s/he is likely to object. For example, it would be within a person's expectations that their details will be used by MPS Care to respond to a request for information about the services they have enquired about. However, it would not be within their expectations that MPS Care would pass their details onto a third party for marketing purposes.

MPS Care will process personal data in accordance with all applicable laws and applicable contractual obligations. More specifically, MPS care will not process personal data unless at least one of the following requirements are met:-

a. The data subject has given consent to the process of their personal data for one or more specific purposes
b. Processing is necessary for the performance of a contract to which the data subject is party or to take steps at the request of the data subject prior to entering into a contract
c. Processing is necessary for compliance with a legal obligation to which the Data Controller is subject
d. Processing is necessary to protect the vital interest of the data subject or of another natural person
e. Processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the Data Controller
f. Processing is necessary for the purposes of the legitimate interest pursued by the Data Controller or by a third party (except where such interests are overridden by

the interests or fundamental rights and freedoms of the data subject, where the data subject is a child).

There are some circumstances in which personal data may be further processed for purposes that go beyond the original purpose for which the personal data was collected. When deciding as to the compatibility of the new reason for processing, guidance and approval must be obtained from the Data Protection Officer before any such processing may commence.

In any circumstance where consent has not been gained for the specific processing in question, MPS Care will address the following additional conditions to determine the fairness and transparency of any processing beyond the original purpose for which the data was collected:-

- Any link between the purpose for which the personal data was collected and the reasons for intended further processing
- The context in which the personal data has been collected, regarding the relationship between data subject and the Data Controller
- The nature of the personal data, whether Special Categories of Data are being processed or whether personal data related to criminal convictions and offences are being processed
- The possible consequences of the intended further processing for the data subject
- The existence of appropriate safeguards pertaining to further processing, which may include anonymization or pseudonymization (using anonymous, alternative names)

6.2. Special Categories of Data

MPS Care Group will only process Special Categories Data (also known as sensitive data) where the data subject expressly consents to such processing or where one of the following conditions apply:-

- The processing relates to personal data which has already been made public by the data subject
- The processing is necessary for the establishment, exercise or defense of legal claims
- The processing is specifically authorized or required by law
- The processing is necessary to protect the vital interest of the data subject or of another natural person where the data subject is physically or legally incapable of giving consent
- Further conditions, including limitations, based upon national law related to the processing of genetic data, biometric data or data concerning health.

In any situation where Special Categories of Data are processed, prior approval must be obtained from the DPO and the basis for this processing clearly recorded with the personal data in question.

Where Special Categories of Data are being processed, MPS Care will ensure that suitable protection measures are in place to protect the data.

6.3. Childrens Data

Children are unable to consent to the processing of personal data. Consent must be sought from the person who holds parental responsibility over the child. However, it should be noted that where processing is lawful under other grounds, consent need not be obtained from the child or the holder of parental responsibility.

Should MPS Care foresee a business need for obtaining parental consent, relating to processing personal data of a child, guidance and approval must be obtained from the DPO. An example of where we would need to process consent is the use of photos or video footage where a child is included.

6.4. Data Quality

MPS Care will adopt all necessary measure to ensure that the personal data it collects and processes is complete and accurate in the first instance and is updated to reflect the current situation of the data subject.

The measures adopted by MPS Care to ensure data quality include:-

- Correcting personal data known to be incorrect, inaccurate, incomplete, ambiguous, misleading or outdated, even if the data subject does not request rectification.
- Keeping personal data only for the period necessary to satisfy the permitted uses or applicable statutory retention period.
- The removal of personal data if in violation of any Data Protection principles or if the personal data is no longer required.
- Restriction, rather than deletion of personal data, insofar as:
    - A law prohibits erasure
    - Erasure would impair legitimate interest of the data subject
    - The data subject disputes that their personal data is correct and it cannot be clearly ascertained whether their information is correct or incorrect.

6.5. Profiling and Automated Decision-Making

MPS Care will only engage in profiling and automated decision-making where explicit consent has been given or where it is necessary for the performance of a contract with the data subject or where it is authorized by law.

Where MPS Care utilizes profiling and automated decision-making, this will be disclosed

to the relevant data subjects. In such cases the data subject will be given the opportunity to:-

- Express their point of view
- Obtain an explanation for the automated decision
- Review the logic used by the automated system
- Supplement the automated system with additional data
- Have a human carry out a review of the automated decision
- Contest the automated decision
- Object to the automated decision-making being carried out.

MPS Care must also ensure that all profiling and automated decision-making relating to data subject is based on accurate data.

6.6. Digital Marketing

MPS Care will not send promotional or direct marketing material through digital channels such as mobile phones, email and the internet, without first obtaining consent.

Where consent has been given to use personal data for digital marketing purposes, the data subject must be informed at the point of first contact that they have the right to change their mind or object to having their data processed for such purposes. If the data subject puts forward an objection to digital marketing, processing of their personal data must cease immediately. The records must be updated to reflect their opt-out decision, rather than being completely deleted.

It should be noted that where digital marketing is carried out in a 'business to business' context, there is no legal requirement to obtain consent, provided the person is given the opportunity opt-out.

6.7. CCTV

MPS Care uses CCTV systems for crime prevention and detection in some homes. To comply with data protection law and the Information Commissioners Code of Practice, all sites with CCTV system installed must:-

- -only use the system for crime prevention and detection i.e. not to watch staff unless it relates to a crime
- Ensure that the videos only cover MPC Care homes i.e. not roads, pathways or property outside of the boundaries
- Have signage in visible locations stating:
    - MPS Care Group is the Data Controller
    - The system is used for crime detection and prevention
    - The contract telephone number is 01773 5466736

- The system must be password protected
- Monitors must be turned off when not being used
- The camera quality should be crisp and clear
- There must be processes for extracting sections of the recording with all personal data not relating to the data subject being blurred
- The recording should be restricted to a rolling 30 days.

7. DATA RETENTION

To ensure fair processing, personal data will not be retained by MPS Care for longer than necessary in relation to the purposes for which it was originally collected for which it was processed.
The length of time for which MPS Care needs to retain personal data is set out in MPS Care 'Data Retention Schedule'. This considers the legal and contractual requirements, both minimum and maximum, that influence the retention periods set forth in the schedule. All personal data must be deleted or destroyed as soon as possible where it has been confirmed that there is no longer a need to retain it.

8. PROTECTING THE DATA

MPS Care will adopt physical, technical and organizational measure to ensure the security of personal data. This includes the prevention of loss or damage, unauthorized alteration, access or processing and other risks to which it may be exposed by human action or the physical or natural environment.

The minimum set of security measures to be adopted by MPS Care is provided under the Information Governance under the GDPR Policy.

9. DATA SUBJECT RIGHTS

The DPO will establish a system to enable and facilitate the exercise of data subject rights:-

- Right to be informed
- Right of access
- Right to rectification
- Right to erasure
- Right to restrict processing
- Right to data portability
- Right to object
- Rights in relation to automated decision making and profiling

All requests for Right of Access (or Subject Access Request) must be directed to the DPO. Each request will be logged as it is received. Appropriate verification must confirm that the requestor is the data subject or his/her authorized legal representative. A completed response to each request must be provided within one calendar month of the receipt of the identity verification or the written request from the data subject if no identity verification is required. If the request is made electronically the information shall be provided electronically unless otherwise requested.

If 'Rights of Access' requests are repetitive, vexatious or excessive, the request may be denied.

For more information, see 'Data Subjects Right's Policy'

10. COMPLAINTS HANDLING

In addition to the data subjects' rights, data subjects with a complaint about the processing of their personal data may put forward the matter in writing to the DPO.

An investigation of the complaint will be carried out. The DPO will inform the data subject of the progress and the outcome of the complaint within one calendar month.

11. REPORTING OF POLICY BREACHES

All security incidents much be reported to the DPO by calling 01773 546736, the same day the incident is identified.

12. LAW ENFORCEMENT

In certain circumstances, it is permitted that personal data be shared without the knowledge or consent of a data subject. This is the case where the disclosure of personal data is necessary for any of the following purposes:-

- Prevention or detection of crime
- Apprehension or prosecution of offenders
- Assessment or collection of tax or duty
- Order by a court or by any rule of law
- To aid a Regulator to carry out their activities.

If MPS Care receive a request for personal information from the Police or other law enforcement agencies, the request must be made in writing to the DPO, quoting the legal basis for the request using the relevant forms. The form must quote the Data Protection Act (2018) Schedule 2 part 1.2. Note that requests do not mean that the information must be provided. MPS Care DPO must process all such requests. No information will be provided to agencies

unless it has been reviewed and reacted by the DPO to protect other individuals identified in the documents.

13. REGULATORY EXEMPTIONS

CQC (AND OTHER Regulators – CIW) has power that grants them full access to records in MPS Care services.
Under section 62(2)(b) of the Health and Social Care Act 2008, a person authorized to carry out an inspection on behalf of CQC may access, inspect and take copies of any documents or records held by the service that they are inspecting, where they consider it 'necessary or expedient' to do so for the exercise of CQCs 'regulatory functions'.

In order to exercise these powers, the representative should hold a duty authenticated document showing they have been granted these powers. The 'document' may be printed on rear of the inspectors CQC identity badge or a separate letter of documentation from CQC.

Anyone taking part in a CQC inspection who does not hold such a document cannot and must not attempt to exercise CQCs powers to access medical and care records. However, they may be shown relevant medical and care records where there is a legitimate reason for doing so, e.g. in relation to an investigation.

14. DATA PROTECTION TRAINING

All MPS Care Group colleagues that have access to personal data will have their responsibilities under this policy outlined to them as part of their induction training. In addition, MPS Care will provide regular Data Protection Training and procedural guidance for their employees.

The training and procedural guidance will consist of, at a minimum, the following elements:-

- The Data Protection Principles
- Each staff members duty to use and permit the use of personal data only by authorized persons and for authorized purposes
- The use of procedures and forms adopted to implement this policy
- The correct use of passwords
- The importance of limited access to personal data, e.g. locking computers when leaving desks, ensuring that individual elements of resident's data is only accessible to those who need to access it
- Securely storing manual files, print outs and electronic storage media, e.g. clean desk
- The procedures and safeguards for all transfers of personal data outside of the MPS Care Group network and physical location
- Proper disposal of personal data by using secure shredding facilities
- Any special risks associated with departmental activities or duties.

15. DATA TRANSFERS

MPS Care may transfer personal data to internal departments or third-party recipients. MPS Care may only transfer personal data where one of the transfer scenarios listed below applies and the data subject has been made aware of the transfer:-

- The data subject has given consent to the proposed transfer
- The transfer is necessary for the performance of a contract with the data subject
- The transfer is necessary for the implementation of pre-contractual measures taken in response to the data subjects request
- The transfer is necessary for the conclusion or performance of a contract concluded with a third party in the interest of the data subject
- The transfer is necessary for the establishment in relation to legal claims
- The transfer is necessary to protect the vital interest of the data subject

15.1 Transfers between MPS Care Entities

For MPS Care Group to carry out its operations effectively across its various locations, there may be occasions when it is necessary to transfer personal data from one MPS Care location to another. Should this occur, MPS Care remains responsible for ensuring protection for that personal data.

When transferring personal data to another MPS location:

- Minimum amount of personal data necessary for the purpose of the transfer
- Ensure adequate security measures are used to protect the personal data during the transfer (including password protection and encryption where necessary).

15.2 Transfers to Third Parties

MPS Care will only transfer personal data to, or allow access by, third parties when it is assured that the information will be processed legitimately and protected appropriately by the recipient. Where third party processing takes place, MPS Care will firstly identify if, under applicable law, the third party is considered a Data Controller or a Data Processor of the personal data being transferred.

Where the third party is deemed to be a Data Controller, MPS Care will enter into, in co-operation with the DPO, an appropriate agreement with the controller to clarify each party's responsibility in respect of the personal data transfers.

Where the third party is deemed to be a Data Processor, MPS Care will enter into, in co-operation with the DPO, an adequate processing agreement with the Data Processor. The

agreement must require the Data Processor to protect the personal data from further disclosure and to only process personal data in compliance with MPS instructions. In addition, the agreement will require the Data Processor to implement appropriate technical and organizational measures to protect the personal data as well as procedures for providing notification of personal data breaches.

When MPS Care is outsourcing services to third party providers (including Cloud Computing Services) we will identify whether the third party will process personal data on its behalf and whether the outsourcing will entail any Third Country i.e. non-EU countries, transfers of personal data. In either case, working with the DPO will include adequate provisions in the outsourcing agreement for such processing and Third Country transfers.

The DPO must conduct regular audits of processing of personal data performed by third parties, especially in respect of technical and organizational measures they have in place. Any major deficiencies identified will be reported to and monitored by MPS Care Groups management team.

16. POLICY MAINTENANCE

All enquiries/queries about this policy, including requests for exceptions or charges must be directed to the Data Protection Officer.

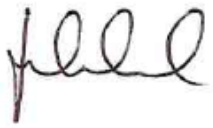
17. RELATED DOCUMENTS

Listed below are documents that relate to and are referenced by this policy:

- Information Governance Policy
- Information Incident Report Procedure
- Subject Rights Procedure
- Privacy by Design
- Confidentiality Policy
- Information Security Policy
- Documents and Records Management Policy
- Information Sharing Policy
- Archiving Policy

Review

This policy should be reviewed on an annual basis.

Signed: 

Date: January 2019

Policy review date: January 2020