DATA PROTECTION POLICY

1. POLICY

1.1. St Philips Care accepts its legal obligation to comply with all appropriate legislation in respect of Data, Information and Information Technology (IT) Security. It also has a duty to comply with guidance issued by the Department of Health (DoH) and guidance issued by professional bodies. St Philips Care is registered with the Information Commissioner's Office.

1.2. All legislation relevant to an individual's right of confidence and the ways in which that can be achieved and maintained is paramount to St Philips Care. This relates to roles that are reliant upon computer systems such as: Service User administration, purchasing, invoicing and care planning. Recent legislation also regulates the use of manual records relating to Service Users, staff and others whose information may be held by St Philips Care.

1.3. This Data Protection Policy (the Policy) aims to detail how St Philips Care meets its legal obligations concerning confidentiality and information security standards. The requirements within the Policy are primarily based upon the General Data Protection Regulation (EU) 2016/679 and the Data Protection Act 2018 (referred to in this Policy as the GDPR) which is the key piece of legislation covering security and confidentiality of personal information.

1.4. For the purpose of this Policy other relevant legislation and appropriate guidance may be referenced. A brief summary of the GDPR, associated legislation and guidelines are detailed in section 2.

1.5. Legislation

There are multiple pieces of legislation which have a bearing upon issues relating to the security and/or confidentiality of personal identifiable information/data. These are detailed in Appendix 2, together with a further 25 Treaties, Directives, Decisions, Proposals, Communications, Green Papers, Conventions, Declarations and Guidelines from the European Union, Council of Europe, United Nations, World Health Organisation and the Organisation for Economic Co-operation and Development.

2. OVERVIEW of Major Legislation

2.1. The GDPR

GDPR applies to all personally identifiable information held in manual files, computer databases, videos and other automated media about living individuals, such as personnel and payroll records, medical records, other manual files, microfiche/film, pathology results, x-rays, closed circuit television recordings etc.

2.2. GDPR dictates that information should only be disclosed on a need to know basis. Printouts and paper records must be treated carefully and disposed of in a secure manner, and staff must not disclose or have access to information outside their line of duty. Any unauthorised disclosure of information by a member of staff will be considered a disciplinary offence.

2.3. GDPR also requires St Philips Care to register its data holdings with the Information Commissioner's Office, identifying the purposes for holding the data, how it is used and to whom it may be disclosed. St Philips Care also has to comply with the principles of good practice known as the Six Data Protection Principles.

2.4. All applications/databases in use within St Philips Care and holding personal identifiable data/information are required under law to be registered for Data Protection purposes. These are registered under St Philips Care's global registration with the Information Commissioner's Office and comply with the GDPR. Compliance will be achieved by adhering the policies of St Philips Care and following the Six Data Protection Principles.

2.5. Under a provision of the GDPR an individual can request access to their information, regardless of the way in which this information may be held/ retained. They may also request correction of inaccurate personal information and removal/destruction (erasure) of their personal data.

2.6. GDPR defines personal data as information that allows a living person to be identified (for example a name, address, location, email, telephone number or even factors specific to the physical, genetic, mental or social identity of that person). Processing is widely defined to mean any collection, recording, storage, sharing or destroying of personal data.

3. DATA PROTECTION PRINCIPLES

There are six principles of good practice within the GDPR. These are normally referred to as the 'data protection principles'.

Principle 1
Personal data shall be processed lawfully, fairly and in a transparent manner

3.1. Lawful basis for processing

It is lawful for us to process people's personal data if one of the following applies

3.1.1. the individual has given us their consent to use their data for specific purpose(s)
3.1.2. processing is necessary to perform a contract with the individual or in order to enter such a contract
3.1.3. processing is necessary for St Philips Care to comply with a relevant legal obligation
3.1.4. processing is vital to protect an individual's vital interests
3.1.5. processing is necessary in order to perform a task in the public interest
3.1.6. processing is necessary in St Philips Care's legitimate interests

We will ideally secure consent from an individual (be they a Service User or employee) to use their personal information or base the use on a contractual obligation or to comply with our legal obligations. Occasionally it will be in St Philips Care's legitimate interest to use data in other circumstances but we will seek to consider the individuals' rights and freedoms under GDPR and seek another basis where possible.

3.1.7. St Philips Care is obliged under the Data Protection requirements and Caldicott recommendations to produce information documentation which is customised to it's own use/s of Service User information.

Staff consent

3.1.8. There are procedures to notify staff, temporary employees (volunteers) etc. of the reasons why their information is required, how it will be used and to whom it may be disclosed. This may occur during induction or by their individual manager.

Service Users consent

3.1.9. Service Users will be made aware of this requirement by the use of the Service Users' Guide and Statement of Purpose; on survey forms and verbally by those health care professionals providing care and treatment.

Principle 2
Personal data shall be collected for specified explicit and legitimate purposes, and shall not be further processed in any manner incompatible with those purposes.

3.2. Registration/Notification

3.2.1. All databases which hold and/or process personal information about living individuals must be registered with the Information Commissioner's Office. This process is known as notification.

3.2.2. A database is any collection of personal information that can be processed by automated means. A few examples are detailed below:-

- Service User records (names and addresses etc.) for invoicing purposes;
- Staff records held on Excel to monitor annual leave and sickness.

3.2.3. This purpose limitation means that St Philips Care will not permit data collected for one specified use to be used in another way (E.g. we will never sell Service User or employee data to a third party or share it unless legally obliged to do so).

Principle 3
Personal data shall be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed

3.3. Information collected from individuals should be complete and should all be justified as being required only for the purpose for which it is being requested. Data minimisation means that no more than the minimum amount of personal data need be kept for specific processing. You should always consider whether it is necessary to write down or record non- essential or peripheral details about an individual.

Principle 4
Personal data shall be accurate and, where necessary, kept up to date

3.4. Accuracy/data quality
Users of software will be responsible for the quality (i.e. Accuracy, Timeliness, and Completeness) of the data they use. This will be achieved by carrying out their own data quality checks and participating as required in St Philips Care's data quality processes.

3.4.1. Staff should check with Service Users that the information held by St Philips Care is kept up to date by asking Service Users / representatives to validate the information held.

3.4.2. Staff information should also be checked for accuracy on a regular basis by the Care Centre Manager.

3.4.3. New GDPR rights oblige St Philips Care to quickly correct data we know to be or are told is inaccurate.

Principle 5
Personal data processed for any purposes shall not be kept for longer than is necessary for those purposes (storage limitation)

3.5. Retention of information

3.5.1. All records are affected by this procedure regardless of the media by which they may be held, stored or retained. HSC 1999/053 provides comprehensive guidance.

3.5.2. If the information on the computer or manual record is not the main record, this is considered to be transient data, and procedures must be put in place to give guidance to these users that the information should be culled, archived or destroyed when no longer deemed to be of use.

3.5.3. Subject to the above, personal data we no longer require should be removed and securely destroyed.

KEEP 3.6 BUT USE ELSEWHERE IN POLICY

3.6. Individual's rights – including subject access/right to complain

Under this principle of the GDPR, individuals have the following rights:-

- right of subject access (further information see below);
- right to prevent processing likely to cause harm or distress;
- right to prevent processing for the purposes of direct marketing;
- right in relation to automated decision taking (profiling);
- right to take legal action for compensation if the individual suffers damage;
- right to take action to rectify, block, erase or destroy inaccurate data;
- right to make a request to the Information Commissioner for an assessment to be made as to whether any provision of the GDPR has been contravened.

Some of these rights still have to be determined by the courts or guidance from the Information Commissioner's Office

Subject Access

3.6.1. Individuals whose information is held by St Philips Care have rights of access to it, regardless of the media in which the information may be held/ retained. Individuals also have a right to complain if they believe that St Philips Care is not complying with the requirements of the Data Protection legislation.

3.6.2. St Philips Care must ensure an up to date procedure is in place to deal with requests for access to information within 30 days of the request.

3.6.3. The Access to Health Records Act 1990 will remain to provide access rights to relatives, or those who may have a claim, to deceased Service Users records.

Compensation

3.6.4. Individuals have a right to seek compensation for any breach of the GDPR which may cause them damage and/or distress.

Complaints

3.6.5. St Philips Care will ensure the complaints procedure is reviewed to take account of complaints which may be received because of a breach or suspected breach of the GDPR.

Principle 6
Using appropriate technical and organisational measures personal data shall be processed in a manner that ensures appropriate security including protection against accidental loss, destruction or damage

Security

3.7. All information relating to identifiable individuals must be kept secure at all times. St Philips Care will ensure there are adequate procedures in place to protect against unauthorised processing of information and against accidental loss, destruction and damage to this information.

3.7.1. Measures should be taken to ensure that:-

- all software and data is removed from redundant hardware and media storage (e.g. tapes, disks) before the hardware is removed from our premises.
- confidential paper waste is shredded or is collected and held in a secure area prior to shredding/incinerating.
- unauthorised viewing of PC screens and charts relating to Service Users' personal information is made difficult or impossible by shutting down PCs when not in use, shielding personal medical information from third parties (for example on boards) and guarding duplicate records adjacent to escape routes.

Disposal of non-clinical waste

3.7.2. St Philips Care has a legal obligation to maintain confidentiality standards for all information relating to Service Users and employees. It is important that this information is disposed of in a secure manner.

3.7.3. All employees will be made aware of how easy it is to breach confidentiality by incorrect use of waste paper, by using examples of 'real life situations' during training sessions. Staff will be informed how to dispose of person-identified waste products.

Disclosure of information/information in transit

3.7.4. It is important that information about identifiable individuals (such as Service Users and staff) should only be disclosed on a strict need to know basis. Strict controls governing the disclosure of service user identifiable information is also a requirement of the Caldicott recommendations.

3.7.5. All disclosures of computer held identifiable information should be included in the relevant data protection registration document.

3.7.6. Some disclosures of information may occur because there is a statutory requirement upon us to disclose e.g. with a Court Order, because other legislation requires disclosure (tax office, pension agency - for staff and notifiable diseases - for Service Users).

3.7.7. If person identifiable information/records need to be transported in any media such as magnetic tape, floppy disc, CD or USB or manual paper records, consider all appropriate measures to remove the possibility of theft or loss (this should be carried out to maintain strict security and confidentiality of this information).

3.7.8. Reliable transport couriers should be used at all times. Packaging should be sufficient to protect the contents from any physical damage during transit, and should be in accordance with manufacturer's specifications.

3.7.9. Contracts between St Philips Care and third parties should include an appropriate confidentiality clause which should be disseminated to the third parties' employees. Contracts should also be considered to allocate the risks of data loss or security breach and third parties' own systems and policies to safeguard personal information entrusted by us should be considered.

3.8. If you need to send person identifiable information in a computer readable format to countries outside of the EEA you must discuss this with the Managing Director or Data Protection Officer as the levels of protection for the information may not be as comprehensive as those in the UK. You may need to check with software suppliers to ensure they conduct any development and bug fixes etc. within the UK or EEA.

STAFF ISSUES

4.1. Training

4.1.1. The Care Centre Manager has overall responsibility for maintaining awareness of data privacy, confidentiality and security issues for all staff. This is carried out by regular supervision sessions covering the following subjects:

- personal responsibilities;
- confidentiality of personal information;
- relevant St Philips Care Policies and Procedures;
- compliance with the six Data Protection Principles;
- individuals rights (access to information and compliance with the principles);
- general good practice guidelines covering security and confidentiality;

4.2. Contracts of employment

4.2.1. Staff contracts of employment are produced and monitored by Head Office. All contracts of employment include a data protection and general confidentiality clause. Agency and contract staff are subject to the same rules.

4.2.2. All employees will be made aware of their responsibilities in connection with the GDPR and other Acts mentioned in this Policy through their Terms and Conditions and targeted supervision sessions carried out by the Care Centre Manager.

4.3. Disciplinary

4.3.1. A breach of this Policy on the Data Protection requirements could result in a member of staff facing disciplinary action.

5. MONITORING & AUDIT

5.1. This policy and associated appendices and procedures will be monitored by the Data Protection Officer and Managing Director.

6. SERVICE USER INFORMATION

6.1. There are specific requirements highlighted within the Caldicott recommendations that apply to service user identifiable information. Most of these are also requirements of compliance with the GDPR. Specifically they relate to security, confidentiality and fair obtaining of information as well as ensuring all disclosures are valid and authorised.

6.2. All Service User information, whether manually or electronically held, will be kept secure when not being used for a Service User care or related purpose.

6.3. Service Users will be made aware of their right of access to their records.

7. STAFF INFORMATION

7.1. Any member of staff current, past or potential (applicant) who wishes to have a copy of their information under the subject access provision of the GDPR will need to contact, in writing, the Managing Director or Data Protection Officer.

8. DISCLOSURE OF PERSONAL PATIENT INFORMATION

8.1. There are Acts of Parliament that govern the disclosure/sharing of personal health information – some make it a legal requirement to disclose and others that state that information cannot be disclosed. These Acts are detailed below:

8.2. Legislation requiring disclosure of personal identifiable information
Public Health (Control of Diseases) Act 1984 & Public Health (Infectious Diseases) Regulations 1998

Education Act 1944 (for immunisations and vaccinations to NHS Trusts from schools)
Births and Deaths Registration Act 1984
Police and Criminal Evidence Act 1984
AIDS Control Act 1987
Anti-Terrorism, Crime and Security Act 2001
Care Standards Act 2000
Children Act 1989

Further detail in these regulations can be found at Appendix 1

APPENDIX 1 OTHER RELEVANT LEGISLATION

1.1. Human Rights Act 2000

This Act became law on 2 October 2000. It binds St Philips Care to respect and protect an individual's human rights. This will include an individuals right to privacy (under Article 8) and a Service User's right to expect confidentiality of their information at all times.

Article 8 of the Act provides that 'everyone has the right to respect for his private and family life, his home and his correspondence'.

Each organisation must act in a way consistent with these requirements. It must take an individual's rights into account when sharing personal information about them.

1.2. Freedom of Information Act 2000

This Act came into force in November 2000. The Information Commissioner (previously the Data Protection Commissioner) will oversee the implementation of this Act. This Act gives individuals rights of access to information held by public authorities. Further information will be available as implementation progresses (see www.dataprotection.gov.uk).

1.3. Regulation of Investigatory Powers Act 2000

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

1.4. Crime and Disorder Act 1998

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

The Act allows disclosure of person identifiable information to the Police, Local Authorities, Probation Service or the Health Service but only if the purposes are defined within the Crime and Disorder Act. The Act does not impose a legal requirement to disclose/exchange person identifiable information and responsibility for disclosure rests with the organisation holding the information.

1.5. The Computer Misuse Act 1990

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

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

1.6. The Access to Health Records Act 1990

This Act gives Service Users' representatives right of access to their manually held health records, in respect of information recorded on or after 1 November 1991. This Act is only applicable for access to deceased persons records. All other requests for access to information concerning living individuals are provided for under the access provisions of the GDPR.

1.7. Access to Medical Reports Act 1988

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

1.8. Other Legislation, Directives, Conventions, Protocols and Agreements etc. governing or applicable to Personal Identifiable information used by Health Organisations.

LEGISLATION	DESCRIPTION
Anti-Terrorism, Crime and Security Act 2001	Repeals the confidentiality restrictions by permitting "any disclosure which can assist any criminal investigation or criminal proceedings being carried out in the UK or abroad which can answer the question whether or not such investigations or proceedings should begin or end." CSCI and Audit Commission would thus be empowered to disclose to the police or other authorities any personal health information they might collect.
Arrangements for Placement of Children (General) Regulations 2011	Relevant to retention of case records.
Births and Deaths Registration Act 1953	Relevant to obtaining, providing and recording personal-identifiable information in registers prescribed by the Registrar General.
Care Standards Act 2000	Relevant to information exchange between agencies involved in the care of vulnerable adults.
Carers (Recognition and Services) Act 1995	Provides for the assessment of the ability of carers to provide care, and for connected purposes - the intention is to give individuals who provide, or who intend to provide, care on a regular and substantive basis a legal right to request to have an assessment of their needs carried out by

	local authorities: i.e. they may request an assessment of the carer's caring ability - to be used in deciding the needs of the person or child requiring care - for the provision of any services.
Children Act 2004	Places statutory obligations on health and local authorities to co-operate.
Civil Evidence Act 1995	Allows for information held electronically to be admitted as evidence in court.
Congenital Disabilities (Civil Liability) Act 1976	Time limits on retention of personal health records.
Consumer Protection Act 1987	Relevant to retention of records.
Copyright, Designs and Patents Act 1988	Makes it illegal to copy computer software without the copyright owner's - or the software developer's permission; places restrictions on the use of copied or converted documents.
Criminal Justice Act 2003	Relevant to retention, custody and destruction of video recordings of child witnesses.
Criminal Justice and Police Act 2001	Gives powers to law enforcement agencies to access and image the contents of any computer system found during a lawful search of premises.
Criminal Justice and Public Order Act 1994	Makes it an offence to procure the disclosure of personal data, to sell information so procured and to offer such information for sale.
Freedom of Information Act 2000	Relates to all public bodies; amends Data Protection Act 1998 and Public Records Act 1958; extends subject right of access to personal information held in unstructured records; gives right of access to corporate information held by public bodies; gives grounds for refusing or exemption from disclosure.
Health Act 2006	Relevant to co-operation between NHS bodies and between NHS bodies and local authorities by requiring such co-operation; governs obtaining information, defines restrictions on and makes criminal offences of unlawful or reckless disclosure of personal-identifiable information in relation to the activities of the Commission for Health Improvement and the Health Service Commissioners; covers provision of information relevant to the registration of a birth; amends Health Act 1977.
Health and Safety at Work Act 1974 and Regulations on the Reporting of Injuries, Diseases and Dangerous Occurrences 1985 SI 2023 and 1989 SI 1457	Relevant to notification of industrial accidents and diseases.
Health and Social Care Act 2008 and Health Service (Control of Patient Information) Regulations 2002	Gives definitions for "patient information and "confidential patient information"; gives Secretary of State for Health powers to make regulations allowing or forbidding the disclosure of personal-identifiable and other information and making such disclosure or non-disclosure mandatory on health organisations and health professionals without the need for individual consent in a variety of possible situations.
Health Service Commissioners Act 1993	Relevant to confidentiality of personal-identifiable information.
Limitation Act 1980	Specifies time limits on retention of records relevant to the time within which a civil action may be brought through the courts.
Mental Health Act 2007	Relevant to disclosure to and by approved social workers to enable them to assess service users and makes provisions relating to relatives and "nearest relatives" requiring health and local authorities to co-operate in the provision of after care services.

Misuse of Drugs Act 2001 Regulations on the Notification and Supply of Addicts 1971	Relevant to reporting on substance misuse.
Police Act 1997	Relevant to requirements for individuals to disclose information about themselves to third parties - permits disclosure to authorities engaged in: appointments to do with being in charge of young persons, child minding and day care; placing of children with foster parents or approval as a foster parent. Such details may only be requested by registered persons who have applied and been accepted as such under the Act. Any institution can apply to be a registered person if they can say that they regularly need information of this sort for the vetting of persons with which they have dealings.
Police and Criminal Evidence Act 1984	Places a duty on all persons to pass on information to help prevent, detect or prosecute serious crime.
Prevention of Terrorism Act 2005	Gives police and security services powers to require the production of information by any person and makes it an offence to fail to volunteer information.
Public Health (Control of Disease) Act 1984	Requires notification of local authority "proper officer" of persons suffering from a notifiable disease or food poisoning.
Public Health (Infectious Diseases) Regulations 1988	Requires notification to a local authority "proper officer" of persons suffering from a notifiable disease or food poisoning.
Public Interest Disclosure Act 1998	Protects individuals who make certain disclosures of information in the public interest and allows such individuals to bring action in respect of victimisation.
Public Records Act 1958 And Public Records Act 1967	Governs the retention, preservation and destruction of personal health and other records.
The Care Home Regulations 2001	Relevant to retention of records
Road Traffic Act 1991	Relevant to disclosure of information leading to the identification of a person guilty of certain offences.
Regulation of Investigatory Powers Act 2000 and Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000	Redefines law enforcement agencies powers for covert surveillance, phone tapping, email interception etc; grants powers to demand either translation or decryption of encoded traffic and/or the handing over of private keys; affects the introduction of public key infrastructure; introduces new criminal offences relating to failure or refusal to disclose information; permits employers to monitor emails, internet usage and telephone calls by employees with their consent and in certain situations without their consent; restricts rights of employers to use cctv surveillance of staff; makes it an offence to unlawfully intercept public or private telecommunications systems.

Social Security Administration Act 1992	Relevant to disclosure of information relating to particular persons in connection with provisions of community care services by local authorities.
Social Security Fraud Act 2001	Gives Social Security Fraud Investigators powers to access personal information, mainly bank accounts, credit card details, credit ratings etc, but could include employment records or health records, held by organisations where they think a benefit claimant is likely to commit fraud
Supreme Court Act 1981	Relevant to disclosures for litigation purposes where a claim is made in respect of personal injury or death.
Terrorism Act 2000	Relevant to interference with computer systems or information held on computers.
EUROPEAN UNION	
Treaty on European Community	Article 3 on a contribution to the attainment of a high level of health protection Title XII and Article 152 on public health Title XIV and Article 153 on consumer protection
Directive 93/42/EEC of the Council of 14 June 1993	Medical devices
Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995	The protection of individuals with regard to the processing of personal data and on the free movement of such data
Directive 96/9/EC of the European Parliament and of the Council of 11 March 1996	The legal Protection of databases
Directive 97/66/EC of the European Parliament and of the Council of 15 December 1997	The processing of personal data and the protection of privacy in the telecommunications sector
Directive 1999/93/EC of the European Parliament and of the Council of 13 December 1999	A Community framework for electronic signatures
Directive 2000/31/EC of the European Parliament and of the Council of 8th June 2000	Certain legal aspects of information society services, in particular electronic commerce in the internal market
Directive 2002/58/EC of the European Parliament and of the Council of 12th July 2002	Privacy and Electronic Communications
Decision 99/182/EC of the European Parliament and of the Council of 22 December 1998	Concerning the fifth framework programme of the European Community for research, technological development and demonstration activities
Decision 99/168/EC of the Council of 25th January 1999	Adopting a specific programme for research, technological development and demonstration on a user-friendly society (1998 - 2002)

Proposal COM(1998)518 of 10 September 1998	For a European Parliament and Council Decision adopting a Multi-annual Community Action Plan on promoting safer use of the Internet
Communication COM(1994)347 19 July 1994	Europe's way to the information society - an Action Plan
Communication COM(1997)570 18 November 1997	The follow-up to the Green Paper on the protection of minors and human dignity in audio-visual and information services including a proposal for a Council Recommendation concerning the protection of minors and human dignity in audio-visual and information services
Green Paper COM(1998)585 of 20 January 1999	Public sector information in the information society: a key resource for Europe
COUNCIL OF EUROPE	
Convention 108 28 January 1981	The protection of individuals with regard to automatic processing of personal data
Recommendation R(97)5 13 February 1997	The protection of medical data
UNITED NATIONS 14 December 1990	UN Guidelines concerning computerised personal data files adopted by the General Assembly
WORLD HEALTH ORGANISATION 1994	Regional Office for Europe Declaration on the promotion of patients' rights in Europe