POLICY DOCUMENT

Policy Title:	Information Governance
Policy Group:	Whole Organisation
Policy Owner:	Information Services Manager
Issue Date:	25 August 2021
Review Period:	1 year
Next Review Due	25 August 2022
Author:	S Burchell
Cross References:	Health Records Policy; Admission Transfer and Discharge of Patients Policy; Mobile Computing and Social Media Policy; Acceptable Use of Wi-Fi Services Policy; Patients' Guide, Information for Patients Policy; Internal Communications Policy; Human Rights Act 1998; Common Law Duty of Confidentiality; General Data Protection Regulation; Data Protection Act 2018
Evidence:	IGA Records Management Code of Practice for Health and Social Care 2016 Data Security and Protection Toolkit 2019-2020 GMC Confidentiality Oct 2009 CQC The Right Information Sept 2009 CQC Essential Standards Dec 2009 CQC Safe Data, Safe Care 2016 CQC Retention Policy Statement 2012 NHS Destruction and Disposal of Sensitive Data: Good Practice Guidelines 2012 EU General Data Protection Regulation 2016 NHS Care Record Guarantee 2011 BMA Access to Health Records: Guidance for Health Professionals in the United Kingdom 2014
How implementation will be monitored:	Routine Audits and reports to Management Team NHS Digital Data Security and Protection Toolkit
Sanctions to apply for breach:	If appropriate retraining. Wilful or negligent breach will be considered as a disciplinary matter and can result in prosecution for an offence under the General Data Protection Regulation or other applicable legislation, or an action for civil damages under the same Act.
Computer File Ref.	O:\risk management\Policies\Whole Organisation\Information Governance Policy 2020
Policy Accepted by MT	25th August 2021
Sign-off by CEO	

Statement of purpose

This policy sets out how information is to be handled in terms of acquisition, storage, disclosure and destruction in order that the standards required by Regulation can be maintained concerning record keeping, confidentiality and security. Holy Cross Hospital recognises that good information management is an essential part of patient care, corporate governance and human resource management. Information in this context includes Patient and Personnel Records (including personally sensitive information) and records required for legal purposes, to comply with regulations and demonstrate compliance. There is much legislation and regulation governing Information Management and this policy aims to provide a practical guide for the purposes of Holy Cross Hospital. However it cannot provide detailed information covering all aspects. Employees and other staff must be prepared to seek advice from a member of Management Team if any matter is unclear.

Roles and Responsibilities

The following table sets out the roles and responsibilities of Hospital managers and staff

Job Title	Responsibe for
Chief Executive	Definition of policy, implementation of policy throughout organisation, arranging audits and identifying and assessing risks affecting Information Management. Assigned as the Information Governance Lead.
Director of Clinical Services	Overseeing management of healthcare records and acts as Caldicott Guardian to assure high standards of confidentiality of personal sensitive information
Finance Manager	Manages financial and insurance records and archives and oversees work of and Administration staff.
Human Resources Manager	Manages Human Resources records and archives and conducts regular audits to assure integrity of data held
General Manager	Manages records relating to buildings, building services, supplies, Health and Safety, and the work of housekeeping, maintenance and catering staff
Information Services Manager	Oversees safekeeping of patient and corporate records archive, oversees use of Hospital computer network and and is responsible for security and back-up. Maintains information asset register. Arranges updates to Hospital website. Arranges and reports on audit of this policy. Ensures Patient Guide is maintained in all relevant locations in up-to-date form. Assigned as Senior Information Risk Owner, and is responsible for compliance with the NHS Digital Data Security and Protection Toolkit self-assessment.
Learning & Development Coordinator	Deputy for IT in the absence of the Information Services Manager. Assigned as Data Protection Officer.
All staff including employees, contractors, volunteers	To be aware of their responsibilities with regards to safe management of hospital records; use of computers and accessing information available via server and internet; and ensuring the confidentiality of all personal sensitive information to which they have access.

Policy Statement

The manner in which data is acquired, stored, used and disposed of is governed by laws and regulations which apply to everyone working at or for the hospital.

The following principles for dealing with Information Management and Data Disclosure are drawn from the laws and regulations listed in appendix 1. These are general principles to apply to all information pertaining to Holy Cross Hospital, the patients, staff, volunteers, sub-contractors and their employees working on-site and those in possession of information about Holy Cross Hospital. Subject-specific information will be found within the Procedures section. The Hospital is committed to complying with Level 2 of the HSCIC Information Governance Toolkit.

1 Legal Basis for Processing Special Categories of Personal Data

Holy Cross Hospital processes special categories of data for the purposes of healthcare and employment. Article 9(2)(h) defines the exemption from the prohibition on processing sensitive data if it is necessary for the purposes of preventive or occupational medicine, for the assessment of the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment or the management of health or social care systems and services on the basis of Union or Member State law or pursuant to contract with a health professional and subject to the conditions and safeguards referred to in Article 9(3). Article 9(3) specifies that such processing may be legally undertaken under the supervision of a medical professional subject to obligations of professional secrecy. In the context of Holy Cross Hospital healthcare is undertaken under the supervision of Registered Nurses and Chartered Physiotherapists subject to obligations of professional secrecy under the Nursing and Midwifery Council and the Chartered Society of Physiotherapists respectively.

Under Schedule 1 Part 1(2) of the Data Protection Act 2018 processing of personal data may be undertaken for health or social care purposes, subject to the provisions and safeguards of Article 9 of the GDPR.

Article 9(2)(b) of the General Data Protection Regulation defines the exemption from the prohibition on processing sensitive data if it 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. Article 88 of the General Data Protection Regulation sets out the basis for the processing of employment-related data under national law. Under Schedule 1 Part 1(1) of the Data Protection Bill 2017, processing may take place if it is necessary under Employment, Social Security, or Social Protection Law.

Limited amounts of non-sensitive personal data are processed for the purposes of marketing and administering of educational courses delivered by the Hospital. This data is processed under Article 6(1)(f) where such processing is necessary for the purposes of legitimate interests pursued by the Hospital.

2 Confidentiality

Holy Cross Hospital will take all reasonable steps to maintain complete confidentiality of all personal information. Therefore, all persons at Holy Cross Hospital are required to take due care at all times to ensure the confidentiality of patient information. Personal information must be used only by the persons and for the purposes that it was originally intended. Holy Cross Hospital does not make the names and addresses of patients or relatives available to other organisations or individuals

unless required to do so by regulation or order of a court or with the patient's prior approval.
When dealing with sensitive data, including personal information about patients, their relatives and staff, staff must:

- collect or retain information only if it is necessary to fulfil a specified purpose;
- store and maintain this information as securely as the situation allows and whenever possible anonymise it.;
- access, copy or disclose this information only to fulfil a specified purpose;
- ensure that information is not retained longer than is required to fulfil a specified function or by statutory requirements and that it is destroyed completely and in a controlled manner.

Disclosures of confidential information or disclosures of any data of a personal nature can result in prosecution for an offence under the General Data Protection Regulation or an action for civil damages under the same Regulation.

The Director of Clinical Services has been designated as the "Caldicott Guardian" with particular responsibility for ensuring the security of personal sensitive information about patients. (see Appendix 1 for information about the Caldicott principles.)

3 Data Acquisition

In collecting any personal data, written or verbal there must first of all be a defined need which must be explained to the individual concerned (or their representative) and their permission to obtain, retain and disclose that information should be obtained whenever it is reasonably possible to do so. They must also be made aware of the limitations which apply to the Hospital's proposed use of that information and their rights under the General Data Protection Regulation. This is best done in writing with written acknowledgement from the individual that they have been informed.
Consent does not have to be obtained for processing data acquired from a third party if that consent is disproportionately difficult to obtain.

4 Data Storage

All personal information must be kept securely and adequate precautions taken to protect it against risks such as unauthorised access, loss and fire. Access to the information must be on a need-to-know basis, controlled and restricted to authorised personnel only. Personally identifiable information from written and computerised records must not be divulged or taken off site without explicit permission from management. Hard copy personally identifiable information is kept secure in locked cabinets, in locations that are locked when unstaffed. Ward office doors are secured by electronic keypads.

The Hospital maintains an Information Asset Register that records assets in the form of hardware, software and services. (see M:\administration\Information Governance\Toolkit Docs\Asset register and
m:admin:computer network:users meeting:system admin:ITassets).

5 Electronic Records

Electronic records are included in the General Data Protection Regulation. The Hospital's computer system is protected from unauthorised access by hardware and software protection and there is a comprehensive back-up system in place. Potential new users will be assessed by the Information Services Manager. The Information Services Manager will conduct an induction session will all new users prior to username and password being issued. Individuals with permission to access the system receive a written statement regarding the General Data Protection Regulation and other relevant legislation and sign a Computer User Agreement. A User Account is created for them on the system to which they specify a unique password.

Computer users must recognise a special responsibility to maintain the integrity of the data protection systems in place without which the safety and security of confidential information may be at risk. The safeguards include hardware measures (turning off computers when not in use) and software (use of passwords, automatic locking of unattended workstations, virus checking, firewall and other protection to the server).

6 Data Disclosure including Subject Access Requests

Personal sensitive information that is identifiable to an individual may not be disclosed to a third party without the individual's express written permission having been obtained in advance.

Permission is not required to disclose anonymous information. However, there must be no possibility of a link being made back to an individual so, for example, identifying information by a person's initials and date of birth is not acceptable.

Care Quality Commission and NHS Clinical Commissioning Groups: These bodies acting in their official capacity as regulators or purchasers of services for patients may require the disclosure of information without obtaining the explicit consent of the "data subject". The reason for requiring such disclosure must be clearly stated and in the event of any doubt, the advice of the Senior Information Risk Owner (Information Services Manager) should be obtained.

Disclosing information to the individual: Paragraph 63 of the General Data Protection Regulation entitles an individual (the data subject) to request from a data controller a copy of the information constituting personal data about him or her. If the individual wishes the Hospital to disclose such information, he or she (or someone authorised by them) must state in what records or other information they wish to see or have copied. A response will be given within one calendar month. No charge may be applied for any copies, except in the case of manifestly unfounded, excessive or repeated requests; any charge will be based upon the administrative costs of providing such information. The Information Services Manager is responsible for dealing with all such requests and will make reference to the provisions of the GDPR and guidance issued by the Information Commissioner on matters of detail.

Criminal Investigation: Information may be disclosed without the data subject's consent to the police or to a Court with a view to investigating or preventing criminal activities.

Amending data in a record: The data subject or their authorised representative, may request that data that is believed to be erroneous be corrected. Such correction should be made in such a way that the original entry remains legible with the time and date of the alteration recorded. The opinion or judgement of a health professional recorded in a health record must not be altered or deleted. However, it is acceptable for the patient or their authorised representative to state that they disagree with the opinion written. If dissatisfied the patient may make a formal complaint or take their case to the Information Commissioner.

7 Data Transmission

Careful consideration must be given to the means by which information is transmitted. In particular it is not considered that email is a secure means when there is no approved method of encrypting data. The Hospital has access to a set of nhs.net email accounts issued by NHS Digital and administered by Holy Cross Hospital Information Services, and this is the only approved method for emailing patient information. Accounts are available to managers, therapists, senior nurses, and other staff as required. Accounts must be approved by a member of Management Team.

The Hospital operates a “safe haven” arrangement for fax receipt. Faxes marked “confidential” and addressed to “safe haven” re handled only by Reception staff who place the transmission in an envelope, seal it and arrange for it to be delivered as soon as possible to the person designated as the recipient.
Any documents containing confidential data sent out of the Hospital must be sent to a fax number that operates similar procedures to ensure the confidentiality of the data transmitted.

All staff must take care when making or receiving telephone calls that there is no possibility of disclosing confidential information unintentionally. The use of cordless or mobile phones requires particular attention.

8 Use of Email

A Hospital Outlook 365 email account ending with @*holycross.org.uk* is issued to all members of staff after an appropriate settling period, usually within 3 months of starting. Email may be accessed via both Hospital-owned and personal equipment including PCs, laptops, smartphones, tablets etc. Any personal equipment accessing Hospital email must be encrypted and this will be checked by the Information Services Manager or his deputy prior to installation of Hospital email on personal equipment.

It is an employee’s responsibility to check their email at least once per day at the start of their shift.

Inappropriate use of email may lead to problems such as distraction, time wasting and legal claims. This policy sets out the Hospital’s position on the correct use of the e-mail system (see also section D6 of the Staff Handbook).

Authorised Use
The e-mail system is available for communication on matters directly concerned with the legitimate business of the Hospital.

All e-mails must comply with Hospital communication standards. Patients should not be directly identified in Hospital email. The accepted method of referring to patients in Hospital (holycross.org.uk) email is by initials combined with room number – for example AB123. Confidential email discussions regarding patients should be carried out via NHS email accounts instead.

E-mail messages and copies should only be sent to those for whom they are particularly relevant.

E-mail should not be used as a substitute for face-to-face communication. “Flame-mails” (e-mails that are abusive) must not be sent. Hasty messages, sent without proper consideration, can upset and cause concern or misunderstandings.

Virus hoaxes and chain letters should not be forwarded. Email messages that warn of a new unstoppable virus that will immediately delete everything from the computer are usually hoaxes. These warnings should never be passed on without checking with the Information Services Manager first. This also applies to chain emails.

Offers or contracts transmitted via e-mail are as legally binding on the Hospital as those sent on paper.

Laws relating to written communication also apply to e-mail messages, including the laws relating to defamation, copyright, obscenity, fraudulent misrepresentation, freedom of information, and discrimination.

E-mails containing frivolous, libellous, abusive, defamatory, offensive, racist or obscene remarks should not be sent or forwarded, even if they are meant to be a joke. Such emails are discourteous and offensive, may break the law, and could be forwarded to external email addresses.

Unsuitable e-mail or attachments should not be sent, especially anything of a sexual nature.

Replies to spam (junk e-mail) should not be sent. Replying to spam or unsubscribing confirms that an email address is 'live', which generates more spam. Such emails should just be deleted.

External messages or attachments should not be copied without permission. Copyright laws might be infringed if permission is not received first.

Unknown files or messages should never be introduced into the system without first being checked for viruses.

Failure on the user’s part to observe these guidelines could result in disciplinary action, including summary dismissal.

Unauthorised use of email

The Hospital will not tolerate the use of the e-mail system for unofficial or inappropriate purposes, including:

- any message that could constitute bullying, harassment, give offence or other detriment.
- on-line gambling.
- accessing or transmitting pornography.
- transmitting copyrighted information and/or any software available to the user.
- posting confidential information about other employees, the Hospital or its customers or suppliers.

Any unauthorised or inappropriate use of e-mail may result in disciplinary action being taken against the user, which could include summary dismissal.

Implementation of the Policy

Regular monitoring of e-mail messages will be carried out on a random basis. Hard copies of e-mail messages will be used as evidence in disciplinary proceedings.

The Information Services Manager is responsible for the e-mail system and advice on all aspects of the e-mail policy.

Critical information must not be stored solely within the e-mail system. Hard copies must be retained and it is the responsibility of the individual issuing the e-mail to ensure the hard copy is filed. If necessary, documents must be password protected.

Users are reminded that the mere deletion of a message or file may not fully eliminate it from the system.

Users are required to be familiar with the requirements of the General Data Protection Regulation and Data Protection Act 2018 to ensure that they operate in accordance with legal requirements.

If a user has cause for complaint as a result of e-mail communications, they should raise the matter initially with their Manager. If appropriate, the concern may then be raised through the Hospital's Grievance Procedure.

9 Use of Internet:

The Internet is an important communication facility providing contact with professional; governmental and academic sources throughout the world. Where appropriate and duly authorised, staff are encouraged to make use of the Internet as part of their official professional activities.

Staff must not publish any information concerning the business of the Hospital on any Internet site.

The availability and variety of information on the Internet has meant that it can be used to obtain material reasonably considered to be offensive. The use of the Internet to access and/or distribute any kind of offensive material or non-related employment issues, will leave an individual liable to disciplinary action which could lead to dismissal.

The hospital will monitor Internet sites used and visited.

10 Use of personal computing devices

See the Mobile Computing and Social Media Policy.

11 Use of Wi-fi

The use of hospital wi-fi services are covered in the Acceptable Use Policy for Wi-Fi Sevices.

12 Mobile computing

Authorised staff will be issued with mobile computing devices to be used on the Holy Cross LAN Wi-Fi service in line with the Acceptable Use Policy for Wi-Fi Services and the Mobile Computing and Social Media Policy. Staff issued with mobile computing devices are responsible for their device and its security, as summarised in their individual Job Description.

13 Data Destruction:

The General Data Protection Regulation requires that information is not retained for longer than is necessary. This period is calculated from the end of the calendar year in respect of patient records and the current accounting year (March 31st) following the last entry in respect of accounting and personnel records. Records must be retained in usable condition for at least the minimum period.

The table at Appendix 2 defines how long data must be retained before being destroyed. Managers are responsible for ensuring that once files cease to be actively used to accumulate data, they are clearly marked with a suggested date for destruction in accordance with the provisions of this policy. Obsolete electronic data files will be deleted by the Information Services Manager in consultation with the appropriate manager.

Destruction of records will be done so as to maintain confidentiality and will be monitored at all stages. Documents for destruction will be stored securely and their final destruction on site will be supervised by a member of staff authorised in this role by the General Manager.

Destruction of digital media, such as hard drives, magnetic tapes etc., will be contracted to a supplier that will undertake collection and secure destruction in accordance with the BS EN 15713:2009 (magnetic tape, flash drive) and SEAP (hard drive) standards as applicable, and a data destruction certificate obtained.

14 Record Archives

The Hospital will make available secure storage for records that have to be retained but are not required for routine use. Categories include Health, Medicines, Personnel, Administration, Accounts, Health and Safety and Buildings.
Where possible consideration will be given to archiving files in digital form and it is noted that many records except those containing personal sensitive information will be retained in digital form well beyond the minimum retention period.

15 Records without Personal Sensitive Information

The Hospital is required to keep records on a wide range of subjects and also chooses to maintain other records to inform management decision making. These records are collectively referred to as Corporate Governance Records. They constitute a vital resource and require systematic and careful management. Responsibility for this management is devolved to Managers with respect to information in their sphere of management.

Managers in this context are as follows :

- The Chief Executive manages Advisory and Medical Advisory Committee business, Management Team meeting records, external relations, capital works, policy and risk management and legal issues
- Director of Clinical Services for all clinical governance records
- Finance Manager for all accountancy, financial management, insurance and payroll records
- Human Resources Manager for all matters relating to staff, service level agreements and human resources management in general
- General Manager for all records concerning buildings, plant and equipment, health and safety, catering, cleaning and laundry

A fuller reference index to Information Management responsibility is set out in Appendix 2

16 Assessment of New Process, Systems and Services

All proposed new processes, systems and services that involve processing personal data will undergo a risk assessment (Data Protection Impact Assessment) prior to approval.

The Information Services Manager will review the potential impact on information security, confidentiality, data protection and privacy, and information quality and will advise Management Team of any actions required.

17 Audit Arrangements

Audit arrangements will be made to ensure that practice conforms to this policy with reference to clinical, human resources, administrative and accountancy records. Such audits will be carried out at least annually as described in Appendix 4, and the results reported to Management Team.

18 Training Arrangements

Induction: All staff will be given instruction into their responsibilities for maintaining the confidentiality of all information related to patients and their families. Induction training will also deal with security of information including electronic data.

Information Governance training is mandatory annual training for all staff, and is delivered by the Information Services Manager.

Work specific training: Training will be given to clinical, Human Resources, Administration and Accounts staff to enable them to understand and implement the Hospital's policies with regards to Information Management and Disclosure. These policies will be brought to the attention of all medical staff who provide services to patients at Holy Cross Hospital.

19 Incident Reporting

If any member of staff becomes aware that there has been a breach of this policy, the matter should be reported at once to the Information Services Manager using the standard Incident Form.

20 Data Disaster Recovery Plan

Arrangements have been made with a third party for encrypted back-up of data. The Chief Executive, Finance Manager and Information Services Manager have full information about these arrangements and are able to implement the Plan in the event that the Hospital digital data become inaccessible.

21 Equality and Diversity

This policy has been reviewed for overt or implied discrimination within the scope of the Hospital's policies on equality and diversity and none was found.

Procedures

Occupational Health Records: These records are not kept by the Hospital. However data subjects may request access to medical reports provided to the Hospital for employment purposes and any requests for disclosure of information should be made via the Human Resources Department. Such requests are dealt with by reference to the Access to Medical Reports Act 1988. The Act also allows the data subject to withhold consent for medical reports to be provided to an employer.

Disclosure and Barring Service Disclosures: Information about disclosures obtained for employment or voluntary work is set out in the Recruitment Policy.

Accident and Incident Reports

The Hospital is required by contract, insurers, Health and Safety Executive and Care Quality Commission to record details of accidents or incidents. The Accident and Incident Report forms contain personally identifiable information that may also include sensitive information. The forms are to be treated as confidential and must be given to the General Manager who will share the information as required with other managers.

Summarised and anonymised information from the Reports will be entered into a database for aggregating and analysing purposes. Personally identifiable information should not be entered on the database.

Information Incident Reporting Procedure

1. By learning about occasions when there has been a breach of the Information Management Policy that we can steps to prevent a recurrence, improve our procedures and give reports as required by regulation.
2. This procedure applies to all employees and those engaged to work under service level agreement; information incidents may arise from paper or digital records or concern the use of computers, including hardware and software problems.
3. Examples of the types of incident, how they will be managed and reported and any countermeasures:
    a. Loss of clinical records should be reported by the ward sister, therapist or doctor to the Director of Clinical Services and or the Information Services Manager at the earliest opportunity using the Incident form. Precautionary measures include locked filing cabinets, locked rooms, back up of data files.

    b. Unauthorised disclosure by any person that comes to attention of member of staff. Should be reported in same way as a). Measures include staff training and awareness-raising.

    c. Unauthorised downloading of data. Reported as in a). Measures include staff training, security of work-stations and server and password protection of key assets
4. Both management and staff have responsibilities with regards to incident reporting; managers must inform and monitor staff compliance, ensure as far as possible that untoward incidents are recorded and reported, take part in training to remain conversant with systems and participate fully in audit; staff must be familiar with their responsibilities under the Information Governance Policy.
5. Serious information security breaches are required to be reported using the IG Toolkit Incident Reporting Tool.

6. Relevant documentation includes the Information Governance policy, the Computer user agreement, Health Records Policy, Staff Handbook, Acceptable Use Policy for Wi-fi Services, and the Mobile Computing and Social Media Policy.

Register of Electors (see downloaded information in m:admin:reception:lists:register of electors)

The Electoral Registration Office at Waverley Borough Council has advised that all persons normally residing at Holy Cross Hospital at the date the electoral roll questionnaires are received should be included in the return unless they prefer to be registered at another address. The rationale is that the electoral roll is used for other purposes such as to help the police trace a person. The question of whether or not a person has the mental or physical capacity to cast a vote is therefore not relevant.

The following is an extract from Home Office document (see m:reception:lists and records:electoral roll)

5.3 A lack of mental capacity is not a legal incapacity to vote: persons who meet the other registration qualifications are eligible for registration regardless of their mental capacity or lack thereof. Electoral Registration Officers should therefore ensure that persons with learning difficulties or mental health conditions are included in the register of electors.

Patients who at the time of receipt of the enquiry from the Borough Council have the capacity to vote will be assisted, if necessary, to complete the registration form and all communications about the electoral registration of voting will be given directly to them.

For patients who are assessed not to have capacity, the family will be consulted wherever possible and a decision made about whether the patient will be included on the list of electors residing at Holy Cross Hospital. The form for such patients who are to be included on the roll at Holy Cross will be signed by the Registered Manager on behalf of the resident. A copy of any correspondence addressed to the patient following registration will be scanned and retained in the patient's correspondence file (H:patient files:current patients). The Borough Council is instructed not to record patients on the public register, unless the patient or their designated representative instructs otherwise.

To exercise voting rights, a patient must be able to act independently and be deemed to have capacity for this particular task. A note of the decision in each case and on each occasion will be made in the patient's healthcare record.

The Information Services Manager is responsible for providing information on all resident persons to the Electoral Registration Officer and distributing communications or polling cards.

Appendix 1 List of Principal Laws and Regulations

Reference should also be made to NHS Information Governance publications and CQC guidance including DH 079619 Guidance on Legal and Professional Obligations

The Data Protection Act 2018. The Data Protection Act 2018 was passed on 23 May 2018, to bring GDPR within the scope of UK law and to cover those areas formerly covered under the Data Protection Act 1998 that were not included in GDPR..

General Data Protection Regulation. This EU legislation was introduced in April 2016, to be phased in over two years, with a final implementation date of 25 May 2018. From this date is supersedes the Data Protection Act 1998. It provides a single set of data protection rules across the whole of the European Union.

Data Protection (Charges and Information) Regulations 2018. The legislation covers registration with the Information Commissioner's Office and registration charges.

Health and Social Care Act 2008. Holy Cross Hospital is required by regulation under the Health and Social Care Act to maintain records concerning the admission, diagnosis and treatment of patients and also some information about next-of-kin or other significant persons connected with the patient. The Data Protection Regulations require us to obtain consent for processing "sensitive data", which is defined as including health records.

Caldicott Principles. Published in 1997 'The Caldicott Committee: Report on the Review of Patient-identifiable Information', was produced as a result of concerns regarding data flows within, in to and out of the NHS. The report was revised in 2013 with the addition of Principle 7. For a full list of the principles, see the Health Records Policy.

Other Rules and Regulations. There are other Guidelines, Principles and Regulations from professional bodies which apply and professional staff should be aware of them.

Appendix 2

Nature of Record	Where Kept	Period of Retention	Required by	Who is responsible	Method of destruction
Accident Forms and books	Archive Room	8 years following last entry	HSE, CQC	General Manager	Shredding with medical records
Accounts Records	Archive Room	Various – see Accounts list	Auditors	Finance Manager	Batch shredding with medical records
Advisory Committee agendas and minutes	Archive Room	Indefinite	CDoC	CEO	N/a
Audit Trail (patient databases)	Electronic record	Indefinite, except patient data values, to be treated as health record		Information Services Manager	Blanking of patient data values
Building work records	Archive Room	Indefinite or until after demolition of building	CDoC	General Manager	N/a
Clinical Governance audits, minutes etc	Director of Clinical Services or archive	Min 3 years	CQC	Director of Clinical Services	shredding
DBS certificate copies	HR Office	3 years; if subscribed then on file in Personnel records (see below)	CQC	HR Manager	shredding
Drugs Orders	Accounts office	Retain 1 complete year	DH	Finance Manager	Shredding
Drugs Register	Archive Room	2 years following the last entry	DH	CEO	Shredding
Equipment for patient treatment	GM office or archive	3 years following discontinuation of use of equipment	CQC	General Manager	Any appropriate means
Health and safety records	GM or archive room	3 years	CQC	GM	Shredding
Healthcare records	Health Records are to be retained for a period of 8 years following the final entry on the record except in the following instances: • For a patient who was under the age of 17 on the date on which the treatment to which the records refer was concluded, to be kept until the patients 25th birthday. • For a patient who was 17 on the date on which the treatment to which the records refer was concluded, to be kept until the patients 26th birthday. • For a patient who was treated for mental disorder during the period to which the records refer, to be kept for a period of 20 years beginning on the date of the last entry in the record.				

Nature of Record	Where Kept	Period of Retention	Required by	Who is responsible	Method of destruction
	• For a patient who has received an organ transplant, a period of 11 years beginning on the date of the patient's death or discharge whichever is the earlier. • For patients admitted under the terms of a contract, for as long as specified in that contract.				
Information Asset Register	Network resource	Indefinite	IGT	CEO	n/a
In-patient register	Accounts or archive	Indefinite	CQC	Finance Manager	n/a
Insurance Records	Archive room	Indefinite	CDoC	CEO	Not applicable
Learning and development records	HR Office or archive	As HR records	CQC	HR Manager	Shredding
Maintenance Requisition books	Archive room	Retain for 1 complete year following last entry		General Manager	Shredding
Medical Advisory Committee agendas and minutes	CEO or archive	3 years	CQC	CEO	Shredding
Outpatient bookings and attendance records (paper)	Medical Records Archive	2 years		Information Services Manager	Shredding
Patients' Money	Archive Room	12 years following discharge or death of patient		Finance Manager	Batch shredding with medical records
Payroll records	Accounts Office or archive	3 years	Auditors	Finance Manager	Shredding
Personnel records	HR Office or Archive	8 years following retirement, resignation or death of employee	CQC	HR Manager	Shredding
Personnel rosters and records of shifts worked	HR Office	4 years	CQC	HR Manager	Shredding
Policies	Archive or Computer archive	Indefinite	CQC	CEO	n/a
Publications	Archive	Indefinite		CEO	n/a
Register of events that must be notified to Care Quality Commission	CEO	3 years following event (or longer if no sensitive information included)	CQC	CEO	Any appropriate

Nature of Record	Where Kept	Period of Retention	Required by	Who is responsible	Method of destruction
Reports to Management Team	Computer network	3 years			Deletion
Time sheets	Archive Room	3 years	Auditors	Payroll Officer	Shredding
Training session sign off sheets	HR Archive	11 years (3 yr training cycle + 8 yr personnel retention period)		L&D Development Coordinator	Shredding
Vehicle registration documents	Accounts Office	Duration of ownership of vehicle	DVLA	Finance Manager	Shredding
Visitors book and register	Reception/ Archive	3 years		Information Services Manager	Shredding

Appendix 3

Job description clause for users of mobile computing devices

In order to facilitate your duties, you have been issued with a mobile computing device, and may use the wireless LAN connection provided by Holy Cross Hospital on approved Hospital equipment. Sections D4-D7 of the Staff Handbook cover use of Hospital computer equipment, email, internet and confidentiality. You are expected to be familiar these sections, and with the Information Management Policy, the Acceptable Use Policy for Wi-Fi Services, and the Mobile Computing and Social Media Policy. The security of your mobile computer equipment is **your** responsibility:

- Remember that your Wi-Fi enabled device is a gateway to confidential Hospital information.
- Ensure that your portable Wi-Fi enabled device is password-locked when unattended.
- The Information Services Manager must be immediately informed in the event of loss or theft of your mobile device, so that network access from that device may be blocked.
- Wi-Fi allows the use of the Holy Cross network from locations to which members of the public have access. Be aware of your surroundings when viewing confidential information, and close your screen if necessary (physically, or by commanding the device to lock).
- Only authorised staff have access to mobile computing equipment. Do not allow unauthorised personnel to use mobile equipment in your charge;
- You are listed in the IT asset record as the nominated responsible person for your device;
- Store your mobile equipment securely when not in use;
- Obtain authorisation before you remove mobile equipment from the premises;
- Do not store files locally on your mobile device; use an appropriate network drive.
- Do not disable the virus protection software or bypass any other security measures put in place by the Hospital;
- Do not remove personal information off site without authorisation;
- Do not leave mobile equipment unattended in publicly accessible places.
- Ensure that mobile equipment is returned to the Hospital if you are leaving employment.

Appendix 4

Annual audits of information governance are conducted throughout the administrative areas of Holy Cross Hospital, including general admission, equal opportunities and data protection pages of patient files in Ward Offices. Other clinical records were specifically excluded from this audit since they are separately audited in the Health Records Audit.

The aim is to ensure that handling of personally identifiable data is in compliance with the Caldicott Principles and the General Data Protection Regulation.

The audit includes evidence gathered for the Information Governance Toolkit produced by the HSCIC.

- Information map
- Record sets / information assets, with security assessment
- Workstations (AV and C drive storage)
- Check data protection sheet in patient files
- Check admissions forms handwritten vs database generated
- Check audit tables in patient databases
- Check that McAfee client is updating properly on all machines

Information Governance Training

Training attendance records are checked against the current staff list, to produce a percentage attendance and percentage attended in the past year, and identify those staff outstanding for the annual refresher.

Record Sets

Record sets are identified by department, and classified as to whether:
a) They contain no personal identifiable information
b) They contain personal identifiable information
c) They contain personal identifiable information relating to patients
Those records falling under category (a) are logged but no further checks are made.
Those records falling under category (b) are checked against the 6 principals of the General Data Protection Regulation.
Those records falling under category (c) are checked against the 7 Caldicott Principals and the 6 principals of the General Data Protection Regulation.

Information Governance Incidents

A summary of information governance incidents relating to the past year is produced, and any areas of concern flagged for further action.

Patient Database Audits

Both Patient Database are audited for completeness of records and accuracy of information. Analytical tools are used to extract percentage completeness of database fields. For current inpatients, all records are examined; for outpatient databases a sample representing patients that have attended in the past year is examined.

Audit tables recorded on both databases are examined, and record access by user and location summarised. Logs are reviewed for 1) unauthorised access and 2) unusual activity such as record deletions or unwarranted amendments to records.

Patient File Audit
Patient files held in the ward offices were audited against three items.

i) The presence and format of the patient information sheet.
ii) The presence and completion status of the Data Protection sheet.
iii) The presence and completion status of Equal Opportunities monitoring data

IT Asset Audit
An inventory of IT assets is produced and summarised from the IT Assets database. All networked workstations/laptops/tablets etc. are checked to ensure that antivirus software is in place and updating correctly, that USB security software is functioning, that portable devices are encrypted correctly, and for locally stored user documents.

On networked computers, local C: drives were checked for user documents. Documents on C: drive are irrecoverable in the event of deletion or file corruption, since they are not backed up. They are not accessible to colleagues, and in the event of equipment being stolen, are vulnerable to unauthorised access. Where appropriate, all documents found on C: drive are moved directly into the user's personal network P: drive. Exceptions are made for PowerPoint training presentations on laptops; due to the development of the St. Hugh's Education Centre, training is often delivered in a building with no network access, and all laptops are encrypted.

Record Destruction
Record destruction logs are reviewed for compliance with retention periods. An inventory of digital media destruction and status for the past year is produced. This will usually be a record of hard drives removed from equipment, and will record if it is 1) awaiting destruction 2) collected by contractor but data destruction certificates are outstanding and 3) collected by contractor and data destruction certificates received.
All causes for concern will be noted and appropriate action suggested. The audit report will be presented to Management Team and actions approved where appropriate.

Simon Burchell
Information Services Manager
March 2018

Appendix 5

Pseudonymisation and anonymisation

1. Unless absolutely necessary, a patient’s name should not be used as an identifier. The use of a patient’s name is necessary for the care record.

2. When patients are discussed in internal communications, particularly in email, their name should not be used, and an internal identifier used in place of the name. This may be the patient’s internal record number, or room number with initials.

3. In those places where it is practical to do so, the patient’s internal record number should be used in place of the name.

4. When records are used for research purposes, they must be fully anonymised. All identifying information must be removed, and the information passed to the Information Services Manager (SIRO) for approval prior to release. The Information Services Manager will consult with the Data Protection Officer and will either approve the information for release, or request further anonymization, as appropriate.

   In general, name, date of birth, address, full postcode, NHS or hospital number etc. must be removed. Date of birth may be converted to an appropriate age range (e.g. 18-21).

5. Patient Surveys
   These are classified as service evaluation or research and not as clinical audit. As such, patient surveys are a secondary use of patient data, hence care needs to be taken in order to avoid breaching patients’ confidentiality. Surveys will be sent to patients or their nominated representative, with return envelope. Neither the survey nor the return envelope will be marked with any form of identifier, and the survey response will be processed anonymously. Where the respondent identifies themselves, their name will not be included in any further processing, except where a specific response is required.