Trust Policy	Worcestershire Acute Hospitals NHS Trust

Code of Conduct for Employees in Respect of Confidentiality

Department / Service:	Information Governance
Originator:	Information Governance Manager
Accountable Director:	Director of Finance – Senior Information Risk Owner (SIRO)
Approved by:	Information Governance Steering Group Executive Risk Management Committee
Date of Approval:	3rd July 2017
Review Date: **This is the most current document and is to be used until a revised version is in place**	4th December 2020
Target Organisation(s)	Worcestershire Acute Hospitals NHS Trust
Target Departments	All Departments
Target staff categories	All Trust Staff/Contractor/Volunteers

Policy Overview:
All employees and those working on behalf of the Trust are responsible for maintaining confidentiality. This duty of confidentiality is written into employment contracts. Breach of confidentiality of information gained, either directly or indirectly in the course of duty is a disciplinary offence that could result in dismissal. This Code has been produced to protect staff by making them aware of the correct procedures so that they do not inadvertently breach any of these requirements.

Latest Amendments to this policy:
Updated into trust format Update of Personal Identifiable Data (PID) to Personal Confidential Data PCD Added quick reference guide Removed reference to WHITS, Updated email flowchart Updated Social media (5.7) Abuse of Privilege (5.6), and Carelessness (5.8)
4th December 2019 – Document extended for 6 months whilst review process is undertaken

Contents page:

Quick Reference Guide

1. Introduction

2. Scope of this document

3. Definitions

4. Responsibility and Duties

5. Policy detail
- **5.1** Definition of Confidential Information
- **5.2** Requests for Information on Patients
- **5.3** Telephone Enquiries
- **5.4** Requests for Patient Information by Police or Media
- **5.5** Disclosure of Information to Other Employees of the Trust
- **5.6** Abuse of Privilege
- **5.7** Social Media
- **5.8** Carelessness
- **5.9** Use of Internal and External Post
- **5.10** Faxing
- **5.11** Storage of Confidential Information
- **5.12** Disposal of Confidential Information
- **5.13** Clear Desk Process
- **5.14** Confidentiality of Passwords
- **5.15** Access to PC's and Systems
- **5.16** Emailing Confidential Information
- **5.17** Transfer of Personal Confidential Data
- **5.18** Encryption
- **5.19** Registration of Devices
- **5.20** Working at Home
- **5.21** Patients' Rights
- **5.22** Providing Information for Patients
- **5.23** Staff Representatives
- **5.24** Interpretation
- **5.25** Non-Compliance

6. Implementation of key document
- **6.1** Plan for implementation
- **6.2** Dissemination
- **6.3** Training and awareness

7. Monitoring and compliance

8. Policy review

9. References

10. Background
- 10.1 Equality requirements
- 10.2 Financial Risk Assessment
- 10.3 Consultation Process
- 10.4 Approval Process
- 10.5 Version Control

Appendices

Appendix1: Data Protection Act Principles
Appendix2: Caldicott Principles
Appendix3: Contact Details
Appendix4: Social Media Guidance
Appendix5: Discussion Group Guidance
Appendix6: Discussion Group Authorisation Form
Appendix7: Secure Email Routes Diagram

Supporting Documents

Supporting Document 1 Equality Impact Assessment
Supporting Document 2 Financial Risk Assessment

Quick Reference Guide: Code of Conduct in Respect of Confidentiality

All employees working in the NHS, including temporary staff such as all contractors, voluntary staff, and students are bound by a legal duty of confidence to protect personal information they may come into contact with during the course of their work. This is not just a requirement of their contractual responsibilities but also a requirement within the Data Protection Act 1998, the NHS Code of Practice on Confidentiality 2003, any other appropriate professional codes of conduct and the Caldicott Principles

All employees are responsible for maintaining the confidentiality of information gained during their employment by the Trust. This duty continues after termination of employment. Any breaches of this code could lead to disciplinary action or dismissal.

The Trust is legally required to report and serious incidents/breaches to the police and the Information Commissioners Office and can result in prosecution and fines

To understand your responsibilities and protect patient and staff personal confidential data (PCD) ensure you complete your mandatory annual IG training. It is vital that all staff, in particular those who work directly with patient data undertake Information Governance E-learning.

Personal Confidential Data (PCD) is anything that contains the means to identify a person, e.g. name, address, postcode, date of birth, NHS number, National Insurance number etc. Please note even a visual image (e.g. photograph) is sufficient to identify an individual.

Complete your mandatory annual IG training (electronically if you handle patient/staff data)

Keep passwords secure and never share your password

Lock your PC screen when the PC is not in use

Make sure that any computer screens, or other displays of information, cannot be seen by the general public.

If emailing PCD use nhsmail to nhsmail. If either end not nhsmail then the email must be encrypted

Use a Safe Haven fax machines to fax PCD and follow Safe haven guidance

Manager to ensure contractors sign contractor's confidentiality form

Do not leave any medical records or confidential information, including diaries, lying around unattended

Do not dictate patient/staff information in public work areas or public places

Do not discuss patients/staff information when taking telephone calls in public places

Do not talk about patients/staff in public places or where you can be overheard.

Record information accurately, in the right place and at the correct time

Always check letters are sent to the correct patient at the correct address and not containing other patients information

Ensure the correct paperwork is provided to patients such as discharge summaries

It is strictly forbidden to view or discuss any information relating to your own records, or the records of your family, staff or acquaintances unless you are directly involved in their care

Remember it is your responsibility to keep any paperwork which contains patient or staff PCD secure at all times and disposed of in confidential waste.

Handover sheets - nurses must not remove from the wards. Medical staff must remove patient identifiers before removing from the wards.

1. Introduction

All employees working in the NHS, including temporary staff such as all contractors, voluntary staff, and students are bound by a legal duty of confidence to protect personal information they may come into contact with during the course of their work. This is not just a requirement of their contractual responsibilities but also a requirement within the Data Protection Act 1998, the NHS Code of Practice on Confidentiality 2003 and any other appropriate professional codes of conduct. (Appendix 1 – form which must be used when employing any form of contractor).

This means that employees are obliged to keep any personal confidential data strictly confidential e.g. patient and employee records. It should be noted that employees also come into contact with non-person identifiable information which should be also be treated with the same degree of care e.g. business in confidence information such as patient referral letters, discharge summaries, waiting list data, consultant's workloads and clinic lists.

Disclosure and sharing of Personal Confidential Data is governed by the requirements of Acts of Parliament and Common Law of Confidentiality. There are exceptions where it is sufficiently in the public interest to warrant a breach of disclosure, for example in relation to a serious crime or in instances to prevent serious harm or abuse. In these circumstances staff should refer to the Trust's Public Interest Disclosure (Whistleblowing) Policy.

This Code of Conduct for Employees in Respect of Confidentiality does not override the Trust's Public Interest Disclosure (Whistleblowing) Policy.

The principle behind this Code of Conduct (Code) is that no employee shall breach their legal duty of confidentiality, allow others to do so, or attempt to breach any of the Trust's security systems or controls in order to do so.

This Code has been written to meet the requirements of:

- The Data Protection Act 1998
- The Human Rights Act 1998
- The Computer Misuse Act 1990
- The Copyright Designs and Patents Act 1988

Organisations and individuals are responsible for breaches of the Data Protection Act 1998 which can result internally in disciplinary action or in serious cases dismissal and externally in a criminal conviction and fine.

Data Protection Act 1998

There are 8 Data Protection Principles, which regulate the use of person identifiable data (personal data). Any use of personal data should be:

1	Fair and Lawful
2	Used only for specified and lawful purposes
3	Adequate, relevant and not excessive to need
4	Accurate and kept up to date
5	Not kept for longer than necessary
6	Processed in accordance with data subject rights, including rights of access
7	Kept secure and protected against accidental disclosure, loss or damage
8	Not transferred outside the EEA

2. Scope of this document

This policy applies to all employees working in the NHS, including temporary staff such as all contractors, voluntary staff, and students.

Employees are responsible for maintaining the confidentiality of information gained during their employment by the Trust. This duty continues after termination of employment.

3. Definitions

IGSG	Information Governance Steering Group
PCD	Personal Confidential Data
IGTT	Information Governance Training Tool
Datix	Trusts incident reporting system
SIRO	Senior Information Risk Officer
IAO	Information Asset Owner
IAA	Information Asset Assistant
ICO	Information Commissioners Office
Safe Haven	A device or system for sending / receiving PCD securely
Caldicott Guardian	A senior person responsible for protecting the confidentiality of patient and service-user information

4. Responsibility and Duties

4.1 Management Responsibility

The Information Steering Group is responsible for approving and implementing this policy. Managers are responsible for briefing staff regarding the contents of the policy, investigating incidents and ensuring staff complete their annual Information Governance Training.

Managers are responsible for ensuring contractors have signed the Contractors Confidentiality Form before they commence work at the Trust.

Managers are responsible for ensuring staff are informed regarding any personal information that is shared about them with any external agencies

4.2 Staff Responsibilities

This Code has been produced to protect staff by making them aware of the correct procedures so that they do not inadvertently breach any of these requirements. All staff has a duty to understand and comply with this code of conduct.

Any breach of these requirements must be reported as an incident in line with the Trust's Incident Reporting Policy and investigated to an appropriate level.

All confidential breaches reported will be included in bi-monthly incident reports at the Information Governance Steering Group. The Information Governance Manager will follow up actions from the Steering Group and send out staff information on the Trust brief and contact areas directly if required.

All employees are responsible for maintaining the confidentiality of information gained during their employment by the Trust. This duty continues after termination of employment. Any breaches of this code could lead to disciplinary action or dismissal.

Staff need to be aware of their own personal responsibilities with regard to information governance – in particular the Criminal Justice Act 2008 which allows fines of up to £500,000 to be imposed on bodies or individuals who are aware of information risks but have not taken reasonable and appropriate steps to mitigate against those risks**.**

All staff must complete their mandatory annual IG training. Staff whose role involves working directly with patient or staff data must undertake training in Information Governance using the E-learning which is available via the following link;

Click here to go to the Information Governance Training Pages

5. Policy detail

5.1 Definition of Confidential Information

Confidential information can be anything that relates to patients, staff (including non-contract, volunteers, bank and agency staff, locums, student placements), their family or friends, however stored.

For example, information may be held on paper, disc, CD, memory stick, e-mail, computer file or printout, video, photograph or even heard by word of mouth.

It includes information stored on portable devices such as laptops, palmtops, mobile phones, memory sticks and digital cameras.

It can take many forms including medical notes, audits, employee records, etc. It also includes any Trust business confidential information.

Personal Confidential Data (PCD) is anything that contains the means to identify a person, e.g. name, address, postcode, date of birth, NHS number, National Insurance number etc. Please note even a visual image (e.g. photograph) is sufficient to identify an individual.

Certain categories of information are legally defined as particularly sensitive and should be most carefully protected by additional requirements stated in legislation (e.g. information regarding in-vitro fertilisation, sexually transmitted diseases, HIV and termination of pregnancy).

During your work duties you should consider all information to be sensitive, even something such as a patient’s name and address. The same standards should be applied to all information you come into contact with.

5.2 Requests for Information on Patients/Staff

- Staff should never give out information on patients or staff to unauthorised persons who do not “need to know” in order to provide health care, treatment or regarding employment.
- All requests for identifiable information should be based on a justified need and some may also need to be agreed by the Trust’s Confidentiality Lead (Caldicott Guardian). For contact details see Appendix 4.

Any exceptions to this rule may require you to get written consent from the patient or staff member in advance.

If the patient is unconscious and unable to give consent, consult with the health professional in charge of the patient’s care. Click Here for link to GMC Capacity Issues webpage.

Whether you are requesting, using or disclosing confidential information you should at all times abide by the **Caldicott Principles** (see Appendix 3). These are:

- **Justify the purpose of using confidential information**
- **Only use it when absolutely necessary**
- **Use the minimum required**
- **Access should be on a strict need-to-know basis**
- **Everyone must understand their responsibilities**
- **Understand and comply with the law**

- **The duty to share information can be as important as the duty to protect patient confidentiality**

If you have any concerns about disclosing/sharing patient/staff information you must discuss this with your manager and if they are not available, someone with the same or similar responsibilities. Alternatively, if you are uncertain whether disclosure of information can take place please contact the Trust's Confidentiality Lead (Caldicott Guardian).

5.3 Telephone Enquiries

If a request for information is made by telephone:

- Always check the identity of the caller and
- Check they are legally entitled to the information they request.
- Take a number, verify it independently and call back if necessary.
- Never give out information if you are unsure

Remember that even the fact that a patient is in hospital, a patient of the hospital, or is a member of staff, is confidential. If in doubt consult your manager, or the Confidentiality Lead (Caldicott Guardian).

5.4 Requests for Patient Information by the Police, Local Authority Designated Officer (LADO), Solicitors and the Media (unless written permission has been obtained from the patient)

With respect to the Police and Solicitors

- Requests for information from the Police and Solicitors should always be referred to the Head of Legal Services, Legal Services Department, telephone 01527 503867, ext 44600.

With respect to Local Authority Designated Officer (LADO) for safeguarding issues:

- Contact the Safeguarding Team within the Trust on 01905 773871 or ext 39149

With respect to the Media

- Do not give out any information under any circumstances.
- Only Directors/Senior Managers and/or the Communications Department are authorised to do so. If you receive any request from the media by personal visit or by phone refer the person to the Communications Department.

Requests for Staff Information by the Police, Solicitors and the Media (unless written permission has been obtained from the member of staff)

With respect to the Police and Solicitors

- Requests for information from the Police and Solicitors should always be referred to the Head of Legal Services, Legal Services Department, telephone 01527 503867, ext 44600.

With respect to the Media

- Do not give out any information under any circumstances.
- Only Directors/Senior Managers and/or the Communications Department are authorised to do so. If you receive any request from the media by personal visit or by phone refer the person to the Communications Department.

This policy does not take away the rights of a member of staff to discuss their personal employment position with their appointed solicitor or union representative

5.5 Disclosure of Information to Other Employees of the Trust

Information on patients/staff should only be released on a need-to-know basis.

- Always check the member of staff is who they say they are.
- If possible also check whether they are entitled to the information.
- Don't be bullied into giving out information.

If in doubt, check with the consultant/doctor in charge of the patient's care or the Trust's Confidentiality Lead (Caldicott Guardian).

5.6 Abuse of Privilege

It is strictly forbidden for employees to look at any information relating to their own records and their own family, friends or acquaintances unless required for the patient's clinical care or with the employees administration on behalf of the Trust. This includes information held in electronic and paper formats. Action of this kind will be viewed as a breach of confidentiality and may result in disciplinary action. There is a clear process via the Trusts Access to Health Records procedure, where staff can obtain copies of their own clinical records and Subject Access Requests Policy to deal with requests for employment records.

NB Staff must only access / view information which is directly related to the work being undertaken. Even if there is a legitimate reason for access if any member of staff subsequently discusses patient or staff information with other members of staff who are not directly involved in the care or with their family or friends this will be treated as a breach of confidentiality.

If you have concerns about this issue please discuss with your line manager.

5.7 Social Media

Many employees and contractors find it beneficial to share their knowledge and experience with others of similar roles and interests. The trust supports staff in the setting up and use of social media pages for work purposes only, such as twitter or blogs, in order to promote services and engage staff and patients.

The Department of Health in its Digital Strategy encourages these online activities and acknowledges that staff and contractors can improve their personal skills and experience through relevant interactions with others outside the organisation. However staff must be aware that tools provided by third parties do not have equivalent levels of security or availability as tools provided by the department. Examples of third parties are Drop box, Twitter, Yammer, LinkedIn, Google Drive and Ever note.

Therefore staff and contractors must be aware of their personal responsibilities for the appropriate use of social media facilities to support the operational effectiveness of the Trusts business, including its public image, reputation and for the protection of its information assets of all kinds. This involves ensuring confidentiality and maintaining security in accordance with Trust policies and the NHS Information Governance Policy and good practice guidance.

The Trust may take disciplinary action, if necessary, against any staff member who brings the organisation into disrepute by inappropriate disclosure e.g. breaches of the confidentiality, comments or photographs on Trust or personal social networking sites or internet sites.

Appendix 5 provides guidance regarding the correct use of social media. Staff must abide by the guidance provided in this policy and any requirements from their own professional bodies.

Appendix 6 & Appendix 7 provide guidance and a request form to set up a discussion group.

Connecting for Health have also issued some guidance – Click here

5.8 Carelessness

It is every employee’s responsibility to record information accurately, in the right place and at the correct time and to ensure that data is kept confidential and secure at all times.

- Record all data accurately, in the right place and correct time – See Data Quality Policy for more information
- Ensure the correct paperwork is provided to patients such as discharge summaries
- Always check letters are sent to the correct patient at the correct address and not containing other patients information
- Remember it is your responsibility to keep any paperwork which contains patient or staff PCD secure at all times and disposed of in confidential waste.
- Do not leave any medical records or confidential information, including clinical handover sheets or diaries, lying around unattended.
- Make sure that any computer screens, or other displays of information, cannot be seen by the general public.

- Do not talk about patients/staff in public places or where you can be overheard i.e. public transport (including the Park and Ride) and restaurants
- Do not discuss patients/staff information when taking telephone calls in public places
- Do not dictate patient/staff information in public work areas or public places

5.9 Use of Internal and External Post

Best practice with regard to confidentiality requires that all correspondence containing personal information should always be addressed to a named recipient. This means personal information/data should be addressed to a person, a post holder, a consultant or a legitimate Safe Haven, but not to a department, a unit or an organisation. In cases where the mail is for a team it should be addressed to an agreed post holder or team leader. (Refer to the Safe Haven Policy located in the document finder on the Trusts intranet).

Internal mail containing confidential data should only be sent in a securely sealed envelope, and marked accordingly, e.g. 'Confidential' or 'Addressee Only', as appropriate.

External Mail must also observe these rules. Special care should be taken with personal information sent in quantity, such as case notes, or collections of patient records on paper, disc or other media. These should be sent by NHS Courier or by Recorded Delivery, to safeguard that these are only seen by the authorised recipient(s). In some circumstances it is also advisable to obtain a receipt as proof of delivery e.g. patient records to a solicitor.

Generally mail is franked with a return address, but in instances where this does not occur, ensure that a return address is printed on the outside of the envelope to prevent post being inappropriately opened where addresses are incorrect.

Case notes and other bulky material should be transported in the approved containers and never in dustbin sacks, carrier bags, etc. These containers should not be left unattended unless stored, waiting for collection, in a secure area e.g. locked. The containers should only be taken and transported by the approved carrier or hand delivered

5.10 Faxing

Actions to be followed:

- Remove patient identifiable data from any faxes unless you are faxing to a known secure and private area (so-called Safe Havens).
- Faxes should always be addressed to named recipients.
- Always check the number to avoid misdialling and ring the recipient to check that they have received the fax.
- Refer to the Safe Haven Policy on the intranet for more information

If your fax machine stores numbers in memory, always check that the number held is correct and current before sending sensitive information.

5.11Storage of Confidential Information

Refer to the Trust's Records Management Policy.

Paper-based confidential information should always be kept in a secure environment and preferably in a room that is locked, when unattended, particularly at nights and weekends or when the building/office will be un-occupied for a long period of time.

Working diaries can hold a great deal of personal information and should be kept secure when not in use. Precautions should be taken when transporting to ensure it is in your care at all times.

Electronically held confidential information must not be saved onto local hard drives, but onto the Trust's secure network. Where confidential information has to be stored on discs, CDs, memory sticks, microfiche or any other removable media, and then it must be anonymised where possible; password protected and kept in locked storage.

When information is saved to the network, access to that information must be on a strict need to know basis. For further guidance refer to the WHITS Information Security Policy.

The recording, storage and release of CCTV information will be carried out in accordance with the Trust's Management and Operation Code of Practice CCTV Systems and the Operational Procedure for CCTV Control Centres.

5.12Disposal of Confidential Information

Refer to the Trust's Records Management Policy.

When disposing of **paper-based person-identifiable information** or confidential information always use 'Confidential Waste' sacks/cross shredders. Keep the waste in a secure place until it can be collected for secure disposal. Where documents are shredded these can be disposed of in the normal way.

Computer printouts should either be shredded or disposed of as paper-based confidential waste.

Discs/CDs containing confidential information must be either reformatted or destroyed. Computer files with confidential information no longer required must be deleted from both the PC and the server if necessary.

Computer hard disks and mobile devices are destroyed/disposed of by the IT Services.

Fax Cartridges – the waste contents of a fax cartridge (but not the thick inner roll) must be placed in confidential sacks for shredding.

5.13 Clear Desk Process

- All staff should clear their desks at the end of each day.
- In particular all records containing person-identifiable or confidential
- Information must be placed in draws or cabinets
- Unwanted printouts containing person-identifiable or confidential
- Information must be put into a confidential waste bin.
- Discs, tapes, printouts and fax messages must not be left lying around or on devices, but be filed and locked away when not in use.
- This applies to all shared areas as well as desks.
- Sensitive or critical business information must be locked away when not required, especially when the office is vacated.

5.14Confidentiality of Passwords

Personal passwords issued to or created by employees should be regarded as confidential and those passwords must not be communicated to anyone.

- Passwords should not be written down.
- Passwords should not relate to the employee or the system being accessed.
- Passwords should never be shared as the username used to access a system will be considered to match the person accessing the system. Audit trails are available from clinical systems in the case of an incident or complaint showing who and when accessed confidential information.

You will be given more information about password control and format etc. when you receive your training and/or password.

No employee should attempt to bypass or defeat the security systems or attempt to obtain or use passwords or privileges issued to other employees. Any attempts to breach security should be immediately reported to the Countywide Information Security Officer via the IT Helpdesk, and you will also be required to complete an Incident Form. Please be aware this may result in a disciplinary action and a breach of the Computer Misuse Act 1990 and/or the Data Protection Act 1998, which could lead to criminal action being taken against you. (see Appendix 2 for Data Protection Principles).

5.15 Access to PC's and systems

All employees have a duty to ensure that PC's and systems logged into are kept secure. Always lock your PC when you leave it unattended (Ctrl – Alt – Del) to ensure that access to any systems or personal information stored on your H-drive is not open to view or abuse by other staff.

All employees have a duty to not view information to which they are not privy and immediately inform a colleague or lock the PC if they become aware a PC is unattended.

5.16 E-mailing Confidential Information

This will be undertaken in line with the Internet and E-mail Policy. A secure email route diagram (Appendix 8) shows the acceptable areas where sending confidential information from trust email account remain secure. Where sending information outside of these areas, to outside agencies, NHS.net to NHS.net should be used or confidential information should be sent within encrypted attachments.

You should not send information that is patient or staff confidential to an external e-mail address, i.e. outside of the NHS.net community (to an email address that does not end in ‘nhs.net’), without appropriate security measures - this mail must be encrypted – by password protecting documents or using NHS Digital minimum level of encryption which can be requested via the IT Helpdesk.

Patient identifiers should be removed wherever possible, and only the minimum necessary information sent, this may be considered to be the NHS number but no name or address. This in itself can pose problems as the wrong number may be typed.

Special care should be taken to ensure the information is sent only to recipients who have a “need to know“; always double check you are sending the mail to the correct person(s).

Please seek advice from your manager if you are unsure about e-mailing patient identifiable information.

5.17 Transfer of Personal Confidential Data (PCD) & Bulk Data

Personal confidential data can relate to information held about any individual, not just patients and may relate to information about staff, contractors, visitors and members of the public

Patient Identifiable Data is information that allows the identification of an individual patient to be revealed, either explicitly or by implication. It includes:

- Patient’s name.
- Patient’s Address.
- Full post code.
- Date of birth.
- Pictures, photographs, videos, audio-tapes or other images of patients.
- NHS number and local patient identifiable codes.
- Any grouping term such as ‘baby’, ‘new-born baby’.
- Anything else that may be used to identify a patient directly or indirectly. For example, rare diseases, drug treatments or statistical analyses which have very small numbers within a small population may allow individuals to be identified.

Bulk data is defined informally as person identifiable data relating to 51 or more individuals, prioritisation should also consider the impact of losing data e.g. the loss of a lower number of highly sensitive records is likely to have a greater impact than the loss of greater number of less sensitive records.

Any loss of PCD should initially be reported to the IT Helpdesk and an incident form completed, as soon as the loss has been discovered.

Any combinations or use alone of the above list is considered PCD

5.18 Encryption

All devices this includes (but is not restricted to) laptops notebooks, tablets, personal digital assistants (PDA's), palmtops, pagers, USB memory sticks and advanced (3G) mobile phones, must be password protected to prevent unauthorised access to data. Devices holding sensitive information must have pass worded encryption to safeguard against unauthorised access. Encrypted memory sticks are available via WHITS and can be requested via the IT Request Form. Any requirement to store clinical data on mobile devices will need to be agreed by the Caldicott Guardian.

Patient identifiable information should only be stored on mobile devices in exceptional circumstances and should be kept to a minimum (e.g. NHS number or hospital number) wherever possible. Devices holding sensitive information must have pass worded encryption to safeguard against unauthorised access. Any encryption software must be supplied and installed by WHITS, please log with the IT Helpdesk.

5.19 Registration of Devices

All laptops and mobile devices used for NHS business should be registered on the organisations register of mobile devices. This should be maintained and monitored by a Local Laptop Manager (LLM). It is the responsibility of all owners to ensure that their device is registered and risk assessed. Laptops must be registered via the link on the Intranet.

Equipment is approved and issued for the sole use of that individual. Devices must not be passed on to other staff without prior permission of the Local Laptop Manager and their line manager. All such changes must be logged on the device register. Mobile devices must be disposed of in accordance with the WHICTS "IT Disposal Policy".

5.20 Working at Home

It is sometimes necessary for employees to work at their own home. Staff who need to do this would first need to gain approval from their manager. If they agree the following must be considered, remembering that there is personal liability under the Data Protection Act 1998 and Trust contracts of employment for breach of these requirements:

- Ensure the necessary authority to take the records is obtained. This will normally be granted by the line manager.

- When taking manual records it is necessary to ensure there is a record of them being taken, where they are being taken to and when they will be returned.

- Ensure any personal information in manual form e.g. patient/staff files, or electronic format e.g. discs/CDs/memory sticks, are appropriately secured prior to them being taken out of the Trust building(s).

- Make sure they are put in the boot of the car or carried on the person while being transported from work place to home.

While at home staff have personal responsibility to ensure the records are kept secure and confidential. This means that other family members and/or friends/colleagues must not be able to see the content or outside folder of the records.

- No-one must be allowed any access to the records.

If staff take home computer records on a disc, memory stick or CD all of the above apply. Any data that contains PCD must be encrypted. Staff must not, however, load any patient identifiable data onto their own PC.

- Other family members must not be able to access this information.

When taking records back to work this must be carried out securely. For manual records they should be logged as being back within the Trust. For computer records on disc/CD these MUST be virus checked before being loaded onto any of the Trust systems – especially any which can be accessed via the network.

5.21 Patients' Rights

Under the Data Protection Act all patients have a right of access to their records. Patients have a further right to restrict access to their records. For example they may wish to state that they are happy for sensitive information to be shared with one agency but not another. It may be that exercising this right makes the provision of care or treatment difficult or even impossible. Where this is the case the healthcare professional should ensure that the patient is fully aware of the implications of their decision i.e. that the required or most appropriate care and/or treatment cannot be offered. It is ultimately the patient's decision and they must not be put under undue pressure to agree to disclosure regardless of the health professional's own opinion about the need for the information. This needs to be documented within the patient's record and suitable access controls put in place.

A patient has the right to change their mind about a disclosure decision at any time before the disclosure is made.

If unsure please check with the Trust's Confidentiality Lead (Caldicott Guardian).

5.22 Providing Information for Patients

Patients must be informed about the need to disclose information in order to provide high quality care e.g. between members of care teams and between different organisations for their direct health care; and other (possibly less obvious) ways that the NHS uses their information for such essential components of healthcare provision as planning, payment, clinical governance, clinical and financial audits.

Patients should also be informed about other uses, which provide benefits to society – e.g. health surveillance, disease registries, medical research, education and training. As far as possible, information should be anonymised. Where uses are not directly associated with the healthcare that patients receive, staff cannot assume that patients who seek healthcare are content for their information to be used in these ways. Staff must consider whether patients would be surprised to learn that their information was being used in a particular way – if so, then patients are not being informed effectively.

Patients can be given information in a range of ways including leaflets, talking with them, etc., ensuring that any special language or other requirements are met appropriately.

In order to inform patients effectively, staff should:

- Check that patients have received appropriate information. See patient guide: Your Information – What you need to know;
- Make clear to patients when information is recorded or health records are accessed
- Make clear to patients when staff are or will be disclosing information to others (who should be specified);
- Check that patients are informed of the choices available to them in respect of how their information may be used or disclosed; and the possible consequences of their decision;
- Check that patients have no concerns or queries about how their information is used or disclosed;
- Answer any queries personally or direct the patient to others who can answer their questions or provide other sources of information;
- Give information about and facilitate the right of patients to have access to their health records.

If in doubt consult your manager, or the Confidentiality Lead (Caldicott Guardian).

General Provisions

5.23 Staff Representatives

This Policy will not take away the right and responsibility of a Staff Representative to:

- Discuss or form part of a case either within the Trust or with solicitors or speak and discuss with any outside bodies with whoever is deemed necessary in pursuit of their trade union duties always recognising that the confidentiality of individuals must be maintained at all times.

5.24 Interpretation

If any person requires an explanation concerning the interpretation or the relevance of this Code of Conduct in Respect of Confidentiality, they should discuss the matter with their line manager or the Trust's Confidentiality Lead (Caldicott Guardian).

See Appendix 4 for Contact Details.

5.25 Non-Compliance

Non-compliance with this code of conduct by any person working for the Trust may result in disciplinary action being taken in accordance with the Trust's disciplinary policy and may lead, in very serious cases, internally to dismissal for gross misconduct, and external reporting to the police or the ICO

To obtain a copy of the disciplinary policy please discuss with your manager or available on the Trusts intranet pages

6. Implementation

6.1 Plan for implementation

The Information Governance Manager will ensure that this policy is available to all Divisional Managers within the Trust. It is then their responsibility to ensure that all staff groups within their area are directed to this policy. Mandatory Information Governance training covers the confidentiality of information and this is promoted within the trust on a regular basis.

6.2 Dissemination

This policy will be available on the Trust Intranet and a publication in the Trust Brief to inform staff of the update to the policy.

6.3 Training and awareness

Secure transferral of confidential data is covered in the national Information Governance Training

Information Governance Training is mandatory on an annual basis for all staff and is included in the Trusts Training Needs Analysis Appendix A of the Trusts Mandatory Training Policy

7. Monitoring and compliance

Please see the monitoring table on the next page for monitoring and compliance details

Page/ Section of Key Document	Key control:	Checks to be carried out to confirm compliance with the policy:	How often the check will be carried out:	Responsible for carrying out the check:	Results of check reported to: *(Responsible for also ensuring actions are developed to address any areas of non-compliance)*	Frequency of reporting:
	WHAT?	**HOW?**	**WHEN?**	**WHO?**	**WHERE?**	**WHEN?**
Page 7 4.2	Any breach of these requirements must be reported as an incident in line with the Trust's Incident Reporting Policy and investigated to an appropriate level.	Regular monitoring of confidentiality breaches on DATIX	Daily	IG manager	Bi-monthly incident report to Information Governance Steering Group listing incidents	5 times a year
Page 7 4.2	Any breach of these requirements must be reported as an incident in line with the Trust's Incident Reporting Policy and investigated to an appropriate level.	Regular monitoring of confidentiality breaches on DATIX	Daily	IG manager	Quarterly SIRO incident report looking at trends	Quarterly
Page 7 4.2	Compliance with Mandatory Annual Information Governance training	Monthly training dashboard	Monthly	IG manager	Bi-monthly updates to IGSG	5 times a year

8. Policy Review

This policy will be updated every two years by the Information Governance Manager and approved by the Information Governance Steering Group to reflect the Trust's development of policies and procedures and the changing needs of the NHS or when necessary following changes to the law

9. References

References:	Code:
The Data Protection Act 1998	
The Human Rights Act 1998	
The Computer Misuse Act 1990	
The Copyright Designs and Patents Act 1988	
Caldicott Principals	
NHS Code of Confidentiality – November 2003	
Criminal Justice Act 2008	
WHITS Internet and E-mail Access Policy	
Freedom of Information	
Records Management	
IM & T Security	
Research Governance	
Worcestershire Information Sharing Protocol	
Incident Reporting Policy	
Mobile Devices Policy	
New Safe Haven Policy	
IT Equipment Disposal Policy	
Flexible Working Opportunities Policy	
Risk Management Guidance - Social Interaction – Good Practice	

Further Guidance

For further guidance see:

- NHS Code of Confidentiality – November 2003
  www.dh.gov.uk/assetRoot/04/06/92/54/04069254.pdf
- Information Commissioner – Use and Disclosure of Health Data – May 2002

10. Background

10.1 Equality requirements

No impact from the equality assessment (Supporting Document 1)

10.2 Financial risk assessment

No impact from the financial risk assessment (Supporting Document 2)

10.3 Consultation

The policy has been created by the Information Governance Manager with input from the Information Governance Steering Group.

10.4 Approval process

This policy will be approved at the Information Governance Steering Group and at the Policy Working Group (PWG) and sent on the Joint Negotiating and Consultation Committee (JNCC) for information.
The Key Documents Approval Group will then ratify and publish the code

10.5 Version Control

Key amendments to this Document:

Date	Amendment	By:
May 2011	Updated into Trust policy format and change to accountable director – from Director of HR to Director of Finance (SIRO)	Information Governance Manager
Sept 2012	Inclusion of social networking section and updated Confidentially Agreement	Information Governance Manager
June 2013	Incorporated any minor national requirements and updated into new policy template. Updated social media section to reflect current guidance	Information Governance Manager
April 2014	Updated following requests from Human Resources for additional guidance including passwords and secure emailing	Information Governance Manager
April 2015	Updated to include Clear Desk	IG Manager
June 2017	Updated into trust format Update of PID to PCD Added quick reference guide Removed reference to WHITS, Updated email flowchart Updated Social media (5.7) Abuse of Privilege (5.6), and Carelessness (5.8)	Information Governance Manager

Appendix 1

Data Protection Act 1998

There are 8 Data Protection Principles, which regulate the use of person identifiable data (personal data). Any use of personal data should be:

1	**Fair and Lawful**
2	**Used only for specified and lawful purposes**
3	**Adequate, relevant and not excessive to need**
4	**Accurate and kept up to date**
5	**Not kept for longer than necessary**
6	**Processed in accordance with data subject rights, including rights of access**
7	**Kept secure and protected against accidental disclosure, loss or damage**
8	**Not transferred outside the EEA**

Appendix 2

Caldicott Principles

1	Justify the purpose
2	Do not use patient-identifiable information unless it is absolutely necessary
3	Use the minimum necessary patient-identifiable information
4	Access to patient-identifiable information should be on a strict need to know basis
5	Everyone should be aware of their responsibilities
6	Understand and comply with the Law
7	The duty to share information can be as important as the duty to protect patient confidentiality

CONTACTS LIST

WORCESTERSHIRE ACUTE NHS TRUST

Confidentiality Lead (Caldicott Guardian)
Kings Court
Worcester Royal Hospital
Charles Hastings Way
Worcester
WR5 1DD

Information Governance Manager
Kings Court
Worcester Royal Hospital
Charles Hastings Way
Worcester
WR5 1DD

Communications Department
Kings Court
Worcester Royal Hospital
Charles Hastings Way
Worcester
WR5 1DD

Head of Legal Services
Alexandra Hospital
Woodrow Drive
Redditch
B98 7UB

Safeguarding Team
2nd Floor
Charles Hastings Education Centre
Charles Hastings Way
Worcester
WR5 1DD

Appendix 4

Social Media Guidance

Duties and Responsibilities – Private use of Social Media

1. Staff are encouraged not to divulge who their employers are within their personal profile page (e.g. in accordance with the Royal College of Nursing (RCN) guidelines “RCN Legal Advice on using the internet”). However, those that do divulge their employer should state that they are tweeting/blogging etc. in a personal capacity.
2. Staff and contractors are ultimately responsible for their own online behaviour. Staff and contractors must take care to avoid online content or actions that are inaccurate, libellous, defamatory, harassing, threatening or may otherwise be illegal. It is possible for staff or contractors to be subject to civil proceedings or criminal prosecution.
3. Staff and contractors are not authorised to communicate by any means on behalf of the Trust unless this is an accepted normal part of their job, or through special arrangement that has been approved in advance by the Communications Team. No social media sites or pages relating to the Trust should be set up by staff and/or contractors without prior approval from the Communications Team.
4. Staff and contractors who use Social Media must not disclose information of the Trust that is or may be sensitive or confidential, or that is subject to a non-disclosure contract or agreement. This applies to information about service users, other staff and contractors, other organisations, commercial suppliers and other information about the Trust and its business activities.
5. Corporate logos or other visible markings or identifications associated with the Trust may only be used where prior permission has been obtained from the Communications Team.
6. Staff and contractors must not share details of the Trust’s implemented security or risk management arrangements. These details are confidential, may be misused and could lead to a serious breach of security occurring.
7. Staff who may not directly identify themselves as Trust staff members when using social networking sites for personal purpose at home should be aware that the content they post on Social Media sites could still be construed as relevant to their employment with the Trust/NHS
8. Unauthorised disclosure of confidential information would constitute misconduct /gross misconduct in accordance with the Trust’s Disciplinary Policy.
9. When using social networking sites, staff should respect their audience. As a general rule, staff should be mindful of any detrimental comments made about colleagues whilst using Social Media sites, e.g. failing to show dignity at work (harassment), discriminatory language, personal insults and obscenity. These examples are not exhaustive and will be considered a disciplinary matter.
10. The Trust may also take disciplinary action, if necessary, against any staff member who brings the organisation into disrepute by inappropriate disclosure e.g. comments and photographs on social networking sites or personal internet sites.

Duties and Responsibilities - Trust Use of Social Media

The Trust has a corporate presence on Facebook and Twitter and if staff wish to convey news stories, events or messages through these channels, then this must be done via the Communication Team.

Reporting Inappropriate Behaviour on Social Media

If a member of staff or contractor comes across information contained in Social Media sites that contravenes this policy, they should report the issue through the Trust Incident Reporting process.

All incidents will be investigated by the Information Governance or Human resources personnel

Appendix 5

Guidance for setting up and using an on line Discussion Group

If you wish to set up or use an on-line discussion group that will be used for work purposes, then you will need to read the guidance below and complete the form ensuring that it has been authorised appropriately. You must make sure that you are familiar with the Information Governance (IG) rules contained within the Trust's Code of Conduct in Respect of Confidentiality, particularly the information contained under the heading of Social Media.

What is a Discussion Group?

A discussion group is an online forum or message board for individuals to discuss various topics amongst each other. People add their comments by posting a block of text to the group. Others can then comment and respond. Discussion groups differ from chat rooms and instant messaging because they usually deal with one topic and are very often archived. These archives may be organized by topic which means all the messages that reply to a starting message can be read in some order. Participants in discussion groups should realize that what they have to say will be public knowledge for years to come.

Purpose

Discussion groups are a valuable resource to healthcare staff to share their knowledge and expertise in order to improve patient care. However it is imperative that staff follow the Information Governance rules to avoid any confidentiality breaches of patient, staff, or business information.

The Discussion Group membership rules

- One person must act as the Group Account holder
- The Group Account holder must be authorised by their line manager
- Members of the group must be given a copy of this guidance and they must complete an authorisation form. The form must be counter signed by the Group Account holder
- Membership to the group is by invitation only
- Members have to create a user account to allow them to log in and look at the activity log
- Members of the group must ensure that their password is kept confidential and secure at all times
- Passwords should be changed regularly and they should be a minimum of six alphanumeric characters
- The Group Account holder is responsible for ensuring that membership is appropriate and up-to-date
- The Group Account holder will notify the Trust's Information Governance department if the Group Account holder changes
- The Group Account holder will retain all forms confidentially and securely at all times

Confidentiality and Security

Under no circumstances must person identifiable, confidential or sensitive information be shared via the group. This typically includes:-

- Patient's name, address, post code, date of birth, telephone number
- National Insurance Number
- Ethnic Group
- Occupation
- Pictures, photographs, videos, audio-tapes or other images of patients
- NHS number and local patient identifiable codes (e.g. hospital number)
- Anything else that may be used to identify a patient directly or indirectly. For example, rare diseases, drug treatments or statistical analyses which have very small numbers within a small population may allow individuals to be identified.

For further information, advice or guidance please contact a member of the Information Governance Team via the Trust's IG mail box.

Appendix 6

Discussion Group Authorisation Form

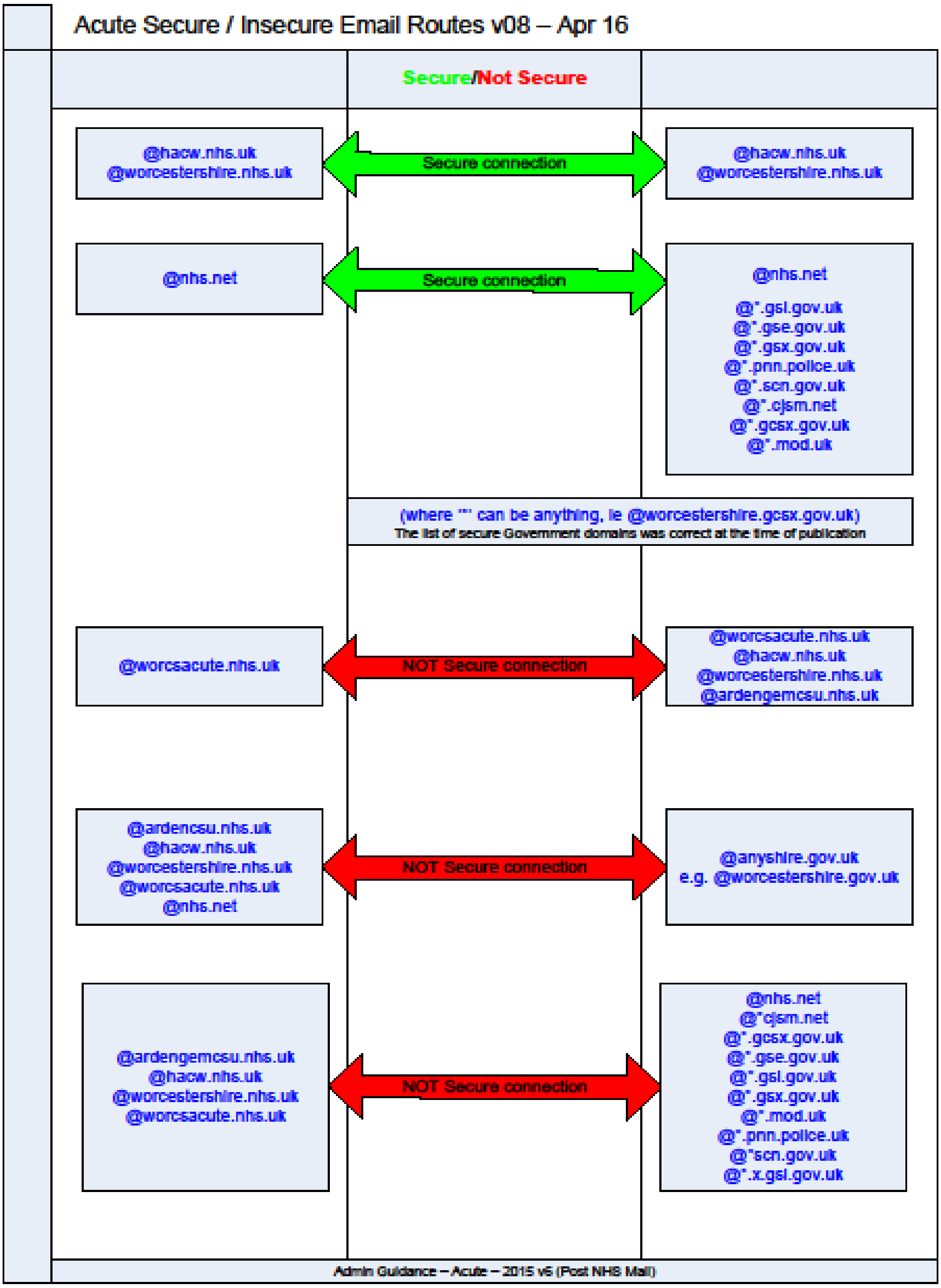
I understand my personal responsibilities under the Data Protection Act 1998 and the NHS Code of Confidentiality 2003 with regard to confidentiality and security. I am familiar with the Trust's Code of Conduct with Respect to Confidentiality and under no circumstances will person identifiable, confidential or sensitive information be shared via the group.

Group Account Holder Details	
Group Account Holder Name:	
Group Account Holder Job Title:	
Group Account Holder Signature:	
Line Manager Name:	
Line Manager Signature:	
Date:	

Group Member's Details	
Name and Type of Group:	
Group Member Name:	
Group Member Job Title:	
Group Member signature:	
Group Account Holder Name:	
Group Account Holder Signature:	
Date:	

The Group Account holder will retain all forms confidentially and securely at all times

Appendix 7



Acute Secure / Insecure Email Routes v08 – Apr 16

Supporting Document 1 - Equality Impact Assessment Tool

To be completed by the key document author and attached to key document when submitted to the appropriate committee for consideration and approval.

		Yes/No	Comments
1.	**Does the policy/guidance affect one group less or more favourably than another on the basis of:**		
	• Race	No	
	• Ethnic origins (including gypsies and travellers)	No	
	• Nationality	No	
	• Gender	No	
	• Culture	No	
	• Religion or belief	No	
	• Sexual orientation including lesbian, gay and bisexual people	No	
	• Age	No	
2.	**Is there any evidence that some groups are affected differently?**	No	
3.	**If you have identified potential discrimination, are any exceptions valid, legal and/or justifiable?**	No	
4.	**Is the impact of the policy/guidance likely to be negative?**	No	
5.	**If so can the impact be avoided?**	No	
6.	**What alternatives are there to achieving the policy/guidance without the impact?**	No	
7.	**Can we reduce the impact by taking different action?**	No	

If you have identified a potential discriminatory impact of this key document, please refer it to Assistant Manager of Human Resources, together with any suggestions as to the action required to avoid/reduce this impact.

For advice in respect of answering the above questions, please contact Assistant Manager of Human Resources.

Supporting Document 2 – Financial Impact Assessment

To be completed by the key document author and attached to key document when submitted to the appropriate committee for consideration and approval.

	Title of document:	**Yes/No**
1.	Does the implementation of this document require any additional Capital resources	No
2.	Does the implementation of this document require additional revenue	No
3.	Does the implementation of this document require additional manpower	No
4.	Does the implementation of this document release any manpower costs through a change in practice	No
5.	Are there additional staff training costs associated with implementing this document which cannot be delivered through current training programmes or allocated training times for staff	No
	Other comments:	None

If the response to any of the above is yes, please complete a business case and which is signed by your Finance Manager and Directorate Manager for consideration by the Accountable Director before progressing to the relevant committee for approval