Information Security Policy

Version:	6
Consultation:	IG Advisory Committee IG & Health Records Committee Senior Information Risk Officer
Ratified by:	Director of Service Delivery
Date ratified:	3 January 2017
Name of originator/author:	John McIlveen
Date issued:	3 January 2017
Review date:	January 2020
Scope	All Trust employees, Governors, volunteers, contractors and Non-Executive Directors

Version	Date	Reason for Change
5	February 2014	Routine scheduled update. Revision to include safeguards re post and email.
6	January 2017	Routine scheduled update. Update names, job titles etc.

1. POLICY STATEMENT

1.1 Everyone working for or on behalf of the NHS has a duty to keep information about patients, carers, clients, staff and other individuals confidential, and to protect the privacy of information about individuals. This duty is enshrined in law, in codes of practice issued periodically by the Department of Health, and in professional codes of conduct.

1.2 It is the policy of the Trust that the measures outlined in this policy should be followed by all employees, Governors, Non-Executive Directors, volunteers and contractors in order that compliance with legislation and good practice can be maintained.

2. INTRODUCTION

2.1 The Information systems used by the Trust represent a considerable investment and are valuable assets to the Trust. The assets comprise equipment, software and data, essential to the effective and continuing operation of the Trust.

2.2 The Trust needs to carefully manage the information provided to it by service users, staff and others as well as that generated for its own use and for third parties. A considerable amount of the data is of a confidential nature, and it is necessary for all information systems to be protected against any events, accidental or malicious, which may put at risk its duty of care, the activities of the Trust or the investment in information.

3. CONTEXT

3.1 The Data Protection Act (1998) defines a legal basis for the handling in the UK of information relating to living people, which includes the requirement to keep such information secure. This duty is reinforced for those who work for and on behalf of the NHS by the Confidentiality: NHS Code of Practice (published 2003).

3.2 The Trust is committed to maintaining and developing an information systems infrastructure that has an appropriate level of security and data protection. All systems must have a security framework appropriate to the level of risk and need for access.

3.3 The intention of information systems security is to ensure an appropriate level of:

- **Confidentiality:** Information is obtained, held and disclosed lawfully and data access is confined to those with specified authority to view and/or change the data.
- **Integrity:** All system assets are operating according to specification and the accuracy of data is maintained.
- **Availability:** Systems and data are available when required and the output from it delivered to the user who needs it, when it is needed.

4. PURPOSE

4.1 The purpose of this policy is:

- To bring to the attention of all staff the need to improve and maintain the security of information systems,
- To advise managers of the approach being adopted to achieve the appropriate level of security.
- To inform staff of their responsibilities under the requirements of relevant legislation, including Data Protection and Human Rights legislation and guidance, and the importance of ensuring the confidentiality of personal and sensitive data.
- To ensure the Trust will comply with current legislation, meet its statutory obligations and observe standards of good practice.
- To minimise the risk of security breach and prosecution.
- To meet the requirements for connection to the NHS network.
- To provide assurance to our patients, staff and others with whom we deal that their personal information is processed lawfully and correctly and held securely at all times.

5. SCOPE

5.1 This policy relates to all types of information within the Trust. These include:

- Patient/Client/Service User information
- Personnel information
- Organisational information.

5.2 This policy covers all aspects of information, including (but not limited to):

- Storage, filing and record systems - paper and electronic
- Transmission of information – e-mail, post, telephone and fax
- Images, including CCTV and photographs

5.3 This policy applies to:

- all information systems purchased, developed and managed by, or on behalf of, the Trust
- All Trust employees (including those on fixed term contracts), non-executive Directors, Governors, contractors and volunteers
- Members of other organisations granted temporary or permanent access (for example to undertake audits or inspections) to confidential information held by the Trust.
- All systems provided by Third Party contractors, where the service has been negotiated on the Trust's behalf e.g. by Department of Health.

5.4 Any appendices to this document shall form part of this policy.

6. DUTIES

6.1 Chief Executive

The Chief Executive has overall responsibility for ensuring that information risks are assessed and mitigated to an acceptable level in his role as Accounting Officer for the Trust.

6.2 Caldicott Guardian

The Caldicott Guardian is responsible for reflecting service users' interests regarding the use of patient-identifiable information and for ensuring that it is shared in an appropriate and secure manner. The Trust's Caldicott Guardian is the Medical Director

6.3 Trust Secretary

The Trust Secretary is responsible for the operational day to day management of all issues relating to information security.

6.4 Managers

Managers have responsibility for ensuring that information within their departments is managed in line with this policy and that staff are aware of and adhere to it. They may also act as Information Asset Owners.

6.5 All staff

All staff have responsibilities for the safe and proper management of information and must adhere to this policy. There is a formal procedure for reporting, investigating and recording information security incidents. Any incidents must be reported via the Datix incident reporting system.

6.6 Senior Information Risk Owner

The Director of Service Delivery is the Senior Information Risk Owner, and provides the focus for the assessment and management of information risk at Board level. The main aspects of the role are:

- to lead and foster a culture that values, protects and uses information for the success of the Trust and the benefit of its service users;
- to own the Trust's overall information risk policy and risk assessment process, test its outcome and ensure that it is used;
- to advise the Chief Executive on the information risk aspects of the Annual Governance Statement;
- to own the Trust's information incident management framework;
- to give prior authorisation to any process requiring bulk electronic data flows containing personal information for more than 50 people

6.7 Information Asset Owners (IAOs)

IAOs are senior members of Trust staff who are responsible for the safeguarding and correct use of information within their team, service or department.

7. DEFINITIONS

7.1 Staff

Within this policy 'staff' is defined as including employees of the Trust, Non-Executive Directors, Governors, volunteers and contractors.

7.2 **Personal Information**

Within this policy personal information is information acquired or held in a professional capacity (e.g for the purposes of delivering care or maintaining employment records) that could be used in isolation or in combination with other items of data to identify a data subject directly or indirectly. It includes such items of data as:

Name, address, postcode, NHS Number, National Insurance Number
Family, Lifestyle or social circumstances
Education and Training details
Employment Details
Financial Details
Photographs and other images

7.3 **Sensitive Personal Information**

Within this policy any of the following data acquired or held in a professional capacity (e.g for the purposes of delivering care or maintaining employment records) are considered to be sensitive data within the Data Protection Act:
Racial or ethnic origin
Political opinions
Religious or other beliefs
Trade union membership
Physical or Mental Health
Sexual life
Alleged offences
Criminal proceeding or convictions

7.4 **Safe Haven**

Although "safe havens" originally referred to the siting of fax machines, the meaning has since been expanded to encompass all secure points at which confidential information is received. Safe Haven procedures ensure that all flows of personal information are received to a secure and protected point.

7.5 **Information Assets**

Information Assets can be defined simply as pieces of information that are valuable to the organisation, such as databases, data files, contracts and agreements, and archived information.

7.6 **Information Asset Owners**

Information Asset Owners are senior members of Trust staff who are nominated to help achieve and monitor a robust Information Governance culture across the Trust, address risks to the information assets they 'own' and to provide assurance to the Information Governance Committee on the security and use of these assets. To do this the IAO must to understand what information is held, how it is used and transferred, who has access to that information and for what purpose. This information must be documented in an information asset register.

8 OWNERSHIP AND CONSULTATION

The Trust Secretary is the author and owner of this policy. The Information Governance and Health Records Committee and the Information Governance

Advisory Committee have been consulted throughout the process of drafting this policy.

9 RATIFICATION

This policy is ratified by the Director of Service Delivery.

10 RELEASE DETAILS

This policy will be published on the Trust's intranet within the Information Governance pages.

11 REVIEW

This policy will be reviewed every 3 years, subject to changes in legislation, advances in technology or the production of national/regional guidance.

12 PROCESS FOR MONITORING COMPLIANCE

12.1 The Information Governance and Health Records Committee will ensure the necessary reviews and updates take place in accordance with changes in national policy or legislation.

12.2 Information security arrangements in a number of locations throughout the Trust will be subject to periodic audit to ensure compliance with this policy. The Information Governance and Health Records Committee and the Information Governance Advisory Committee will receive a regular summary of Information Governance incidents for review and appropriate action.

12.3 An annual IG report will be submitted to the Trust Board's Governance Committee. This report will include information on data protection performance and information security breaches.

13 TRAINING

13.1 Guidance on information security will be produced by the Trust Secretary as required. This will include the creation and maintenance of Information Governance pages on the staff intranet, and associated documentation.

13.2 Training needs will be assessed by the Training Department and appropriate training provided. Such training will normally be delivered through e-learning packages. All new staff will receive Information Governance awareness training as part of their corporate induction, and this includes training and awareness about data protection and information security requirements. Information Governance refresher training, also including data protection and information security, will be a requirement for all existing staff, and will form part of the Trust's suite of statutory and mandatory training. The Delivery Committee monitors compliance with statutory and mandatory training on behalf of the Trust Board.

14 POLICY PRINCIPLES

14.1 Personal and sensitive personal information

14.1.1 Personal information must be treated as confidential unless informed consent is given or special circumstances apply[1]. It is defined as any patient or staff information which is acquired or held in a professional capacity (e.g. for the purposes of delivering care or maintaining employment records) and which would enable that person's identity to be established by one means or another. Generally this is interpreted as name, date of birth and full address but must also include hospital and NHS number. Please remember that combinations such as postcode with date of birth could also be considered to provide identification.

14.1.2 Sensitive or confidential information is regarded as information which, if lost or misdirected, could impact adversely on individuals, the organisation or the wider community. Under the Data Protection Act sensitive personal data is defined as information about a data subject's racial or ethnic origin, political opinions, religious beliefs or beliefs of a similar nature, trade union membership, physical or mental health or condition, sexual life, offences or alleged offences, and information relating to any proceedings for offences committed or allegedly committed by the data subject, including the outcome of those proceedings.

14.1.3 In addition to personal and clinical information, confidential information could include financial information, commercial information and details of any security arrangements, e.g. passwords.

14.1.4 Appendix A sets out procedures for maintaining the confidentiality of confidential information acquired or held in a professional capacity.

14.2 Information Safe havens

14.2.1 Extra vigilance is required in information safe havens where large amounts of personal information is recorded, held or communicated, especially where the information constitutes sensitive personal Information. When unoccupied, the room should be locked and accessible only to authorised staff (perhaps by a coded key pad) and not to all staff working in the building. If sited on the ground floor, any windows should have locks on them. The room should conform to health and safety requirements in terms of fire, safety from flood, theft or environmental damage.

14.2.2 Where frequent transmission of confidential and sensitive information is to take place by fax, then an information safe haven must be set up. Senders should be informed of this and assured that only appropriate people will have access to messages sent. The room should be identified by a sign on the outside of the door or the inside wall marked 'information safe haven'.

15. NETWORK CONNECTION

15.1 All network management controls and procedures will conform to current NHS codes of connection and associated guidance available from the Trust's IT Security Adviser.

[1] More detail about these can be found in the Trust's Data Protection and Confidentiality Policy

15.2 Network Management is the responsibility of Countywide IT Services. All devices connected to the network must meet the required standards. Failure to do so will result in immediate disconnection. No direct connection is permitted between the Trust's Local Area Network (LAN), other LANs or Internet services accessed via public service providers unless authorised and encrypted.

16. ACCESS CONTROL FOR IT SYSTEMS

16.1 Each individual is responsible for keeping their own access password and smartcard secure, and must ensure it is neither disclosed to nor able to be used by anyone else.

16.2 Staff must only access IT systems using their own login and password.

16.3 All staff are accountable for any activity carried out under their login and password. This may be audited. Unauthorised or unlicensed software is not permitted on Trust equipment. It is expressly forbidden for any user to load or operate software gained from the internet, magazines, gifts or other sources, unless authorised by IT Services.

16.4 Access is controlled on the basis of individual user roles and service requirements. Procedures are in place for allocating and controlling access, and passwords.

17. COMPUTER OPERATIONS

17.1 Responsibilities and procedures for the management and operation of all computers and networks will be established, documented and supported by appropriate operating instructions. This refers to both trust wide systems and Directorate/Department based systems.

17.2 Procedures must include: Back-up, media control, event logging, monitoring, protection from theft and damage, unauthorised access and capacity planning.

18. SYSTEMS DEVELOPMENT, PLANNING AND PROCUREMENT.

18.1 Security issues must be considered and documented during all stages of any development projects. Minimum national network connection standards will be incorporated in all new systems.

18.2 New operational software will be quality assured. System test and live data must be separated and rigorously protected.

18.3 All changes to the system must be approved through a formal change control procedure.

19. BUSINESS CONTINUITY PLANNING

19.1 The Trust will put in place a process to develop and maintain appropriate plans for the speedy restoration of all critical IT systems operated by IT services.

19.2 The responsible manager will ensure all systems will have threats and vulnerabilities assessed to determine how critical they are to the Trust.

19.3 Individual departments must have procedures in place to maintain essential services in the event of IT system failure.

20. DESKTOP COMPUTERS AND LAPTOPS

20.1 Each PC or laptop shall have a designated user who will be responsible for the security of that equipment.

20.2 Equipment shall only be specified and purchased via IT Services, in accordance with current recommendations on software and hardware.

20.3 Precautions must be taken to prevent and detect computer viruses. IT Technical Services will provide advice and support on virus control.

20.4 Electronic confidential information must be password protected or encrypted where the PC or laptop is taken off site or is not in a secure area.

21. I-PADS, TABLETS AND SMARTPHONES

21.1 Each i-Pad has a central management system (AirWatch) that allows the Trust to remotely configure settings and record what apps have been installed. It also allows i-Pads to be remotely wiped if required. Staff must not delete this system unless instructed by the Trust's IT Department.

21.2 All iPad apps (whether free or paid for) must be downloaded only via an authorised i-Tunes account.

21.3 i-Pad and smartphone users are responsible for ensuring that equipment is stored securely and locked with a personal passcode when not in use.

21.4 Patient identifiable data must not be transmitted from i-Pads or smartphones without approval from a senior manager or Director.

21.5 iPads and smartphones may be used to record patient consultations for supervision or other purposes provided that a suitable information sharing protocol has been agreed

21.6 Personal i-Pads and personal smartphones should not normally be used to conduct Trust business. However, personal smartphones may be used in exceptional circumstances to conduct Trust business, where no practical alternative exists (for example, when there is no viable signal on Trust-issued equipment while on call). In such circumstances information should be exchanged using the telephone, and the transmission of person identifiable information via email must be avoided.

22. PERSONAL USE

22.1 Reasonable personal use of Trust-owned IT equipment is permitted providing that:

- Such use does not breach the IT Security Policy
- It is used in the employee's own time
- it is used with line management approval
- It is not used in support of a business
- It does not use excessive system resources

- No processing or transmission of person-identifiable information acquired or held in a professional capacity takes place
- Consumables are paid for by the employee
- Files are removed promptly by the employee if requested by the IT Department.

22.2 The Trust's local email service is primarily for business use. Occasional and reasonable personal use is normally permitted provided that this does not interfere with the performance of a member of staff's duties.

22.3 All email is stored centrally and the Trust IT Service may inspect email (including personal email) without notice. Managers must ensure that staff members are aware that the organisation owns the documents they or their colleagues create, and that they do not have intellectual property rights therein.

22.4 Users must not add a personal email account to the main Mail app on their i-Pad or smartphone.

23 STORAGE AND DISPOSAL OF INFORMATION

23.1 All records, reports, printouts or other printed material containing identifiable or confidential organisational information must be treated as confidential and either archived or destroyed securely when no longer needed. Electronic identifiable data must be stored only on devices that have adequate security measures in place. (See Trust IT Security Policy).

23.2 Confidential information, and especially person identifiable information, must not be stored permanently on the 'C' Drive of any PC. This includes the 'My Documents' area of Windows.

23.3 Confidential information, and especially person identifiable information, must not be stored permanently on a laptop or other mobile device, or on removable media such as memory sticks or CDs.

23.4 All data (manual or electronic) must be reviewed periodically to ensure that the information is accurate, up to date and complete.

23.5 Data (manual or electronic) must not be kept for longer than is necessary. The Trust's Records Management Policy provides guidance on minimum retention periods and disposal of records.

23.6 All reports, printouts or other printed material containing identifiable or confidential organisational information, and which has exceeded its retention period, must be disposed of securely through the Trust's confidential waste disposal service. The disposal of computer equipment and devices capable of storing information should be carried out through the IM&T department to ensure all data is removed before disposal.

24 REPORTING BREACHES OF CONFIDENTIALITY AND DATA PROTECTION

24.1 All information governance incidents, including actual and suspected breaches of confidentiality and data protection, must be recorded on Datix and reported to the Trust Secretary.

24.2 The Trust Secretary will review each report and if necessary request an investigation by the appropriate department/manager. Where appropriate, an investigation may be deemed to warrant disciplinary action. This will be the responsibility of the local line manager or the Human Resources Department.

24.3 Serious breaches will be escalated to commissioners and the Information Commissioner as appropriate, using the relevant reporting mechanism. A summary of data losses and breaches will also be included in the Trust annual report.

25. BREACH OF THIS POLICY

25.1 Failure to manage information securely places the Trust at risk of breaching the Data Protection Act 1998, NHS Caldicott Guidelines and Trust policy. All Trust staff have responsibility for the safety and security of the information they process.

25.2 Failure to comply with the terms of this and associated policies may lead to disciplinary action against the individuals concerned.

26. REFERENCES

- The Caldicott Guardian Manual
- The Records Management NHS Code of Practice.
- NHS Information Governance - Guidance on Legal and Professional Obligations
- Data Protection Act 1998.
- The common law duty of confidence.
- Human Rights Act (1998)
- Computer Misuse Act (1990)
- IT Security Policy
- Data Protection and Confidentiality Policy
- E-mail and Internet Policy
- Information Governance Framework Policy
- Disciplinary Policy
- Access to Health Records Policy
- Health and Social Care Records Policy and Procedure
- Business and Corporate Records Retention Schedule
- Health Records Retention Schedule
- Portable IT Equipment Policy

- Social Media Policy
- Confidentiality: NHS Code of Practice
- Health and Social Care Records Policy and Procedures

APPENDIX A –MAINTAINING THE CONFIDENTIALITY OF INFORMATION ACQUIRED OR HELD IN A PROFESSIONAL CAPACITY

1 Laptop

- Confidential information must not be taken off site unless password protected or encrypted[2].
- Where it is necessary to take confidential information off site, remember:
    - Do not leave the laptop unattended unless locked securely
    - Remove confidential information as soon as possible
    - Password protect files containing confidential information
    - Ensure regular housekeeping of laptop files
    - Laptops must not be a primary data store.

2 Computer

- Be careful where you site your computer screen: ensure any confidential or personal information cannot be accidentally or deliberately seen by visitors or staff who do not have authorised access.
- Do not leave Smartcards unattended
- Always keep your password confidential and do not write it down.
- Do not share passwords (use Outlook permissions and shared drives). Sharing passwords may be a disciplinary offence.
- Change your password regularly; most systems will force a regular change of password and designate the format of it.
- Remember to log off your computer when leaving the office, or use password protected screen savers for short absences.
- Any user who suspects their PC may have a computer virus must report it immediately to the IT Service Desk and their manager. To protect other computers, do not transfer any information from the infected PC.
- Any disk or CD coming into the organisation – no matter where it has come from – must be virus checked before use.

3 Removable Media

- Removable media includes memory sticks, CDs, hand held computers (e.g. PDAs), floppy disks etc.
- These devices must not be used for storing personal information on a permanent basis. Use a server instead.
- Trust PCs do not allow files to be saved to non-encrypted USB devices. However read-only access remains possible on non-encrypted devices.
- Devices must always be securely locked away when not in use
- Devices must never be used to transfer confidential information from one site to another unless they are encrypted and password protected. Permission from the Senior Information Risk Owner is required for any transfers involving the personal details of more than 50 people.

2 Encrypt: to change electronic information or signals into a secret code (= system of letters, numbers or symbols) that people cannot understand or use on normal equipment. Encryption software is available to Trust staff.

- No personal information is to be downloaded onto or used on non NHS equipment.

4 Database

- Ensure that any database that is created or introduced to your department/service.is reported to your relevant Information Asset Owner.

5 Telephone

- Be careful about leaving messages on answer phones.
- Be careful when taking messages off answer phones and ensure that messages cannot be overheard whilst being played back.
- Make sure the answer phone volume is low when out of the office.
- When receiving calls requesting personal information:
  - Verify the identity of the caller
  - Ask for a reason for the request
  - If in doubt as to whether information should be disclosed, tell the caller you will call them back. Take advice from your manager.
  - Call back to main switchboard or known and trusted numbers only – not direct lines you do not recognise or mobile telephones

6 Faxing

- Site fax machines away from public areas.
- Use a fax cover sheet that contains a confidentiality statement (Sample Appendix B) .
- Send faxes to named individuals if at all possible and mark them ‘addressee only’.
- Check the fax number is correct before sending. Use pre-programmed numbers or internal numbers where possible and, if there is any uncertainty, send a test sheet through first
- Only send personal information by fax when absolutely necessary. Use identity numbers or initials if they will suffice.
- Do not send more information than is required for the purpose.
- Call the recipient to let them know the fax is about to be sent. Ask them to acknowledge receipt of the fax. If they do not call you, try to call them again.

7 Email

- Confidential or personal information should be sent via e-mail **only if** a secure email link exists. Advice on which email links are deemed secure is available on the Information Governance pages of the Trust Intranet, and from the Trust Secretary. Where no such secure email link exists and the transmission of the data is essential, the data should be encrypted before transmission.

- Before sending any email that contains personal information, you must ensure:
  - the email address is correct, and send a ‘test’ email if you are not sure
  - there is no identifiable data in the ‘subject box’
  - the email is marked ‘confidential’ by clicking on ‘options’, sensitivity’ and then ‘confidential’

- If you receive an email containing information that is sensitive or confidential, or which identifies a person, you must be careful when replying or forwarding it. Even if your own message does not include such information, the original email will still be visible. You should therefore create a new mail message or reply in another way.

7.1 Emails from patients, carers and relatives

- It is increasingly common for patients/service-users and carers/relatives to contact Trust staff by email.

- If a patient/service-user sends you an email, it is important that you make them aware that the system is not secure and check using the following template that they are happy for you to reply by email.

  Thank you for your email.

  Email is not considered a completely secure method of communication. Sending an email is similar to sending a postcard through the ordinary post, which means that it can be read by other people.

  The Trust's policy is that emails should not contain information which is confidential, sensitive or identifies a person without that person's consent.

  Please can you let me know if you would prefer another method of communication.

- If a carer/relative sends you an email about a patient/service-user, you must not include identifiable information in an email without the consent of the patient/service-user. The following template may be used in a reply.

  Thank you for your email.

  Email is not considered a completely secure method of communication. Sending an email is similar to sending a postcard through the ordinary post, which means that it can be read by other people.

  The Trust's policy is that emails should not contain information which is confidential, sensitive or identifies a person without that person's consent.

  As your email is about somebody else, I am not permitted to reply to you by email without that person's consent.

  If you can let me have their consent in writing, I will be glad to reply by email. Otherwise, please can you let me know if you would prefer another method of communication.

7.2 Staff details in emails

- Many emails about members of staff do not contain sensitive or confidential information about them. However, you should always check the contents of an email that you intend to send. If the contents are sensitive or confidential, unless you have the person's agreement to include this information you should remove the person's name or use another method of communication.

8 Post

- Double check the full postal address of the recipient and ensure that the most current contact details are used when sending out letters.
- Ensure envelopes are marked "Private and confidential" when they contain information which is personal and/or sensitive and which may be opened by the addressee or by someone else on their behalf.
- Mark envelopes 'Personal' when the contents are intended for the addressee only.
- Choose an appropriately secure method for sending confidential information through the external post.
- Use a PO Box number as a return address to safeguard patient confidentiality in case the letter is delivered to the wrong address
- Ensure envelopes are properly sealed.
- Do not use internal transfer envelopes for confidential post.
- When necessary ask the recipient to confirm receipt.
- In the rare event of CDs with confidential information being sent by post, they must be encrypted.
- Where a memory stick is used to send confidential information through the post, the memory stick must be one issued by the Trust, and must be password protected
- Do not include details of the sender on the packaging if this may inadvertently disclose a sensitive subject matter to anyone handling the item.
- Where information from clinical systems is required, for example to address letters or issue documentation to service users, you should consider whether the information required can be taken directly from the screen, rather than making a printout.
- Where a printout is necessary you should ensure, before any information is despatched, that the printout can be accounted for and is then securely destroyed via confidential waste.
- Ensure that incoming confidential post is opened away from public areas.
- Appendix C sets out the different forms of post.
- For more detailed guidance on the sending of health records, see the Health and Social Care Records Policy and Procedure.

9 Printer

- You may print confidential/personal information to central smart printers.
- Keep the number of copies to a minimum.
- Remain with the printer until all of the information has been printed.
- If not printing to a smart printer, make sure you select the correct printer.

- Do not leave the printer until you are sure that all your information has been printed.

10 Photocopying

- Do not make excessive copies of confidential information.
- Do not leave the photocopier unattended if you are copying confidential information
- Regularly check /update your distribution list to ensure copies are not sent to staff who have left or moved to another service

11 Bin

- Be sure that you dispose of confidential information appropriately.
- All personal information is confidential and must be shredded or placed in a locked confidential waste bin.
- Confidential waste paper must not be used as scrap paper for messages, notes etc.

12 Filing Cabinet

- Ensure that filing cabinets containing confidential information are always kept locked when not in immediate use. Ensure filing cabinets are not sited in areas which are accessible to members of the public/visitors.
- Ensure regular housekeeping of your files.
- When destroying information, ensure you comply with NHS retention guidelines (NHS Records Management Code of Practice, Part 2).

13 Office

- Remember to lock the office at the end of the day.
- Whenever possible, escort visitors at all times on site.
- Remember to wear your identity badge on-site and always carry it with you at work.

14 Desk

- Operate a “Clear Desk Policy”, especially when hot-desking or working in an open-plan office.
- Do not leave confidential information unattended or out overnight – particularly important when hot-desking or working in an open-plan office.

15 Person

- Ensure you hold confidential conversations in an appropriate place. Inappropriate places include corridors, and at the photocopier!
- If you work in an open plan office, take sensible precautions when holding confidential conversations. Use an empty office or meeting room where possible, and ensure that you cannot be easily overheard.

- Gain the patient's consent before sharing their personal information with relatives.

16 Transport

- If you transport confidential material in a private vehicle or on public transport, make sure that a record is made of its removal from a Trust site. Confidential information must be transported in a case notes bag or other suitable container such as a briefcase. The information should either remain in your sight, or should be locked securely in the boot of your car.

17 Home

- You must not take confidential records home without the express consent of your manager.

18 Help, advice and guidance:

- Ask your line manager
- Contact the e-helpline at 2gnft.Information-Governance@nhs.net

APPENDIX B

2gether
Making life better

2gether
NHS Foundation Trust

Front Sheet for Faxing **Confidential Information**

FOR ATTENTION OF ADDRESSEE ONLY

DATE:

Name of Recipient:	
Fax Number of Recipient:	

Name of Sender:	
Telephone number of Sender:	

Number of sheets being sent including this cover sheet	

This fax is confidential and is intended only for the person(s) to whom it is addressed. If you have received this fax in error, please immediately notify us by the telephone number above and return the message to us by post. If the reader of this fax is not the intended recipient, you are hereby notified that any distribution or copying of the message is strictly prohibited.

APPENDIX C – METHODS OF POSTING INFORMATION

Type	Description	Guidance
Normal Royal Mail post	Relatively insecure. There is no tracking or receipt of items. First class post should reach the recipient within 1 or 2 days.	Suitable for small items, such as appointment letters, test results and general correspondence between health professionals and with patients. Suitable where proof of posting is not needed. Not suitable for sending occasional items about more sensitive matters (such as child protection issues). ALWAYS stamp the envelope with a confidential PO BOX return address.
Royal Mail Recorded Delivery	Suitable for situations where proof of posting and confirmation of receipt are required. This service does not track an item between its being sent and delivered. It is generally as swift as first class post. It requires a signature on receipt and its status can be checked on the internet. This has the benefit over normal post that mail is less likely to be mis-delivered, as the recipient is required to check and sign for the item, and mistakes can be picked up at this stage.	Suitable for large items about one (or few) individuals, such as a request by an individual for a copy of their records or information of higher sensitivity, such as child protection information between organisations. Proof of posting and receipt id important, but damage from loss is relatively small. For example, a loss of a copy of a patient's records is not a permanent loss of the information and, whilst distressing for the individual concerned, the impact is limited to one or two people.). ALWAYS stamp the envelope with a confidential PO BOX return address
Royal Mail Special Delivery	Similar to recorded delivery but offers increased tracking facilities and compensation for loss. It can be swifter than first class post if delivery before 9am is requested and paid for. As with recorded delivery, a signature is needed on delivery and status can be tracked on the internet.	Suitable for large amount of data on individuals or original health records, where proof of postage, tracking during transfer and confirmation of receipt are required. Whilst loss is possible, the risk is reduced as far as possible and there is the potential to narrow down the area of loss. The impact of loss could be high, but using this method reduces its probability. ALWAYS stamp the envelope with a confidential PO BOX return address.
Courier service	To be used where there is an ongoing contractual arrangement detailing the requirements of the service or where there is a 'track and trace' service allowing packages to be tracked and receipted. Delivery time can be specified.	Similar to special delivery but may be faster and more economical for larger items.