DPA01
Data Protection Act
Local Guide

For all staff at

PUBLIC HEALTH INSTITUTE
LIVERPOOL JOHN MOORES UNIVERSITY

Document Reference:	DPA01
Author:	Geoff Webb
Version.Issue:	1.1
Status:	Approved
Approved by:	Dave Seddon
Version date:	November 2017
Review date:	November 2018

Approval and Authorisation

Completion of the following detail signifies the review and approval of this document, as minuted in the senior management group meeting(s) shown.

Version	Authorising Group	Name of Approver	date
1.0	DPA Compliance Group	Dave Seddon	22/10/13
1.0	DPA Compliance Group	Dave Seddon	30/10/14
1.0	DPA Compliance Group	Dave Seddon	28/10/15
1.1	DPA Compliance Group	Dave Seddon	03/11/16
1.1	DPA Compliance Group	Dave Seddon	06/11/17

Document change history

Version	Status	Reason for change	date	Author
0.1	Draft	CPH version of NWPHO doc	04/06/2013	Geoff Webb
1.1	Full	Change CPH to PHI	03/11/2016	Mark Whitfield

Contents

1. Introduction

Public Health Institute's (PHI)'s documented Data Protection Act (DPA) framework ensures that all necessary safeguards are in place and that appropriate use is made of information to ensure high quality of integrity, confidentiality and security.

It covers these areas, which form the sections that follow:

- Information Security and Confidentiality Assurance Framework
- Data protection assurance
- Information security assurance
- Secondary Use assurance
- Corporate information management

This guide provides details of how to access the power point training presentation and also describes how the DPA Framework is put in place; telling you what you need to know, where to find it and who to go to for advice.

1.1 DPA Material - Policies and Procedures

To satisfy the requirements of the DPA, policies and procedures covering all relevant topics are available at http://www.PHI.org.uk/governance

The documentation is listed together alphabetically with a brief description next to each.

At the time of creating this document the following are available:

DPA01 Data Protection Act Local Guide
DPA02 Confidentiality Code of Conduct
DPA03 Information Sharing Agreement
DPA04 Information Security Management Framework (to ISO 27001 level)
DPA05 Incident Policy
DPA06 Information Risk Assessment Process

1.2 Document format

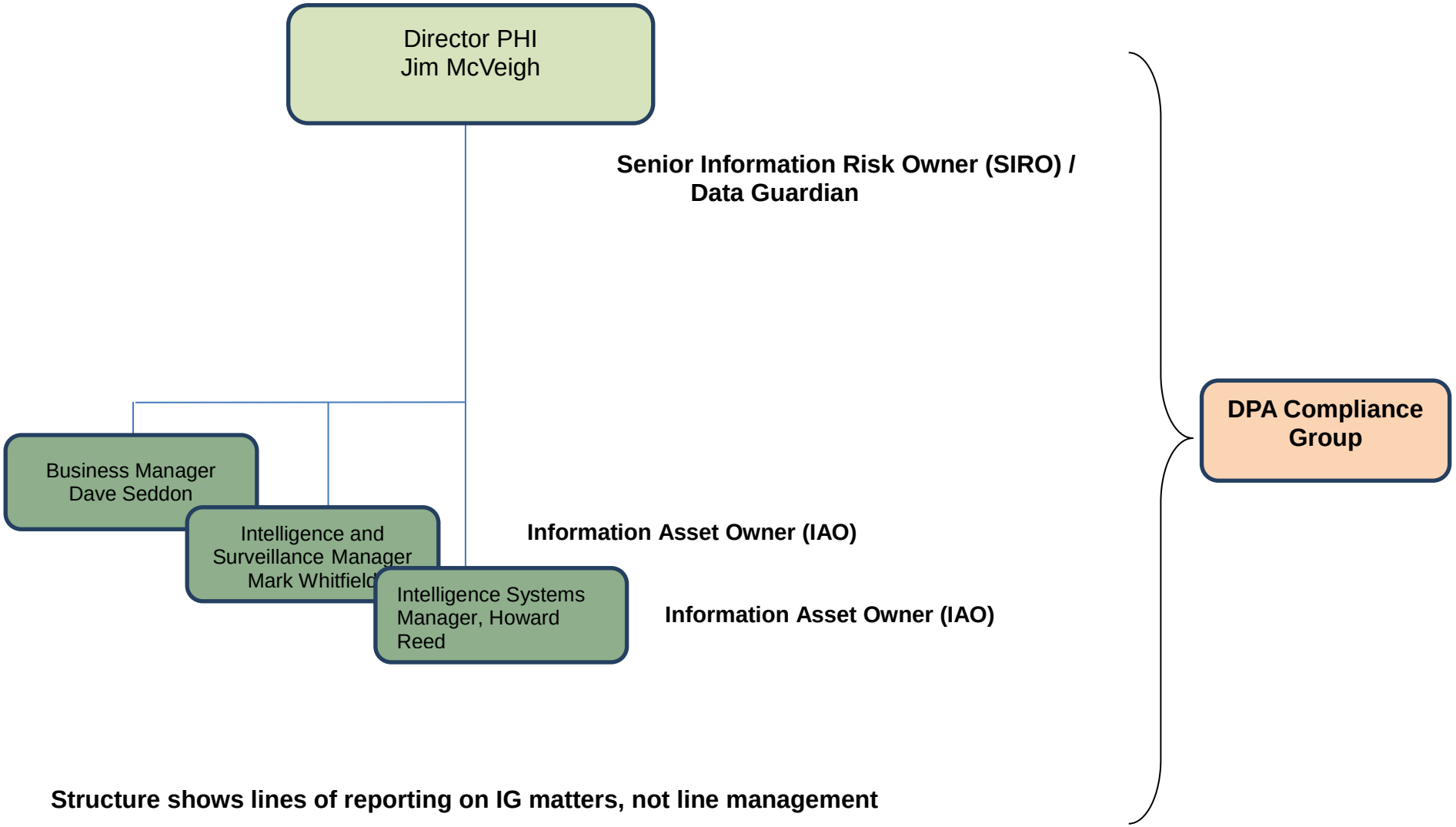
There is a standard format throughout the PHI's DPA documentation so that when you are familiar with it you can find what you are looking for quickly.

Documents are identified by their name, reference number, version, issue and status. The latest version is always on the website but it is possible to find earlier documents in archives on request to the DPA Lead.

2. Information Security and Confidentiality Assurance Framework

2.1 DPA Compliance Group

DPA matters are monitored and discussed at quarterly meetings of the DPA Compliance Group, which has membership including representatives from Business and Systems Development, IT Support, and the PHI Director (chair)
The next page shows the structure of the group.


Director PHI
Jim McVeigh
Senior Information Risk Owner (SIRO) / Data Guardian
DPA Compliance Group
Business Manager
Dave Seddon
Intelligence and Surveillance Manager
Mark Whitfield
Information Asset Owner (IAO)
Intelligence Systems Manager, Howard Reed
Information Asset Owner (IAO)
Structure shows lines of reporting on IG matters, not line management

2.2 Roles & Responsibilities to be updated

2.2.1 Data Guardian

PHI's Data Guardian has a particular responsibility for reflecting staff and individuals' interests regarding the use of identifiable information and is responsible for ensuring such information is stored, used and shared in an appropriate and secure manner, in accordance with the rights of individuals.

2.2.2 Senior Information Risk Owner (SIRO)

The SIRO is designated lead responsibility for the organisation's information risks and provides a focus for the management of information risk at the highest level.

2.2.3 Information Asset Owners (IAO)

The SIRO is supported by IAOs, who are involved in running the relevant business. Their role is to understand what information is held, what is added and what is removed, how information is moved, who has access and why.

As a result they are able to understand and address risks to the information assets they 'own' and to provide assurance to the SIRO on the security and use of the assets. They are responsible for registers of Information Assets in their areas.

3. Data protection assurance

All staff must comply with the Data Protection Act, which is not simply something we should do, it is a legal requirement for us all to comply. In summary form, the principles we must comply with are described below.

3.1 Data Protection Principles

We must comply with the eight Data Protection principles designed to protect the rights of individuals whose personal data we process:

Principle 1 – Personal data shall be processed fairly and lawfully and in particular shall not be processed unless specified conditions can be met.

Principle 2 – Personal data shall be obtained only for one or more specified and lawful purposes and shall not be further processed in any manner incompatible with that purpose or purposes.

Principle 3 – Personal data shall be adequate, relevant and not excessive in relation to the purpose or purposes for which they are processed.

Principle 4 – Personal data shall be accurate and where necessary kept up to date. We can't work safely with the wrong information.

Principle 5 – Personal data processed for any purpose or purposes shall not be kept any longer than is necessary for that purpose or those purposes.

Principle 6 – Personal data shall be processed in accordance with the rights of data subjects, taking into account European laws, Human and Civil Rights Acts.

Principle 7 – Appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of or damage to personal data. We must take care of personal information.

Principle 8 – Personal data shall not be transferred to any country or territory outside the European Economic Area, unless that country or territory ensures an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data.

3.2 Person Identifiable Data (PID)

- Person Identifiable Data (PID) is information about a person which would enable that person's identity to be established
- The term applies to staff as well as individuals
- A small number of items together could allow the person to be identified, mainly name, address, date of birth, but also postcode, telephone number, NHS or staff reference, or medical records number.

Whenever we handle these we must take great care.

3.3 PHI Computer Systems Access

All staff have access to one or more of the PHI computer systems, accessed with a user-id and a password.

There are strict rules about the structure and use of passwords, including the fact that you must never share your password with anyone else. To do so will result in disciplinary action that could include dismissal.

You must protect all passwords and access devices and never let someone else use yours. Full details are in the DPA04 Information Security Management System document at http://www.PHI.org.uk/governance

Remember that access to computer systems is only to be given to people who have been trained and are authorised to use them.

3.4 Information - Keep it to yourself

- **Clear Screen Policy** - Never leave personal information displayed on a screen for unauthorised people to see

- If you have to leave the screen unattended, keep it secure by doing Ctrl-Alt-Del to log off or lock your PC
- **Clear Desk Policy** - Any confidential information must be placed out of sight, in locked cabinets when not in use. This includes any portable computers that may contain confidential information
- Safeguard portable computers when travelling and when using out of the office – always transport them out of sight to help stop them being stolen.

3.5 Portable Storage Devices (USB etc.)

Thousands of USB sticks are lost or stolen each year causing personal, sensitive and confidential data to be lost or, more worryingly, exposed. The Information Commissioner, who monitors how we all follow the Data Protection Act principles, has been granted the ability to impose high fines for those who breach any of the rules. Fines can be up to £500,000.

To ensure that your data is secure, PHI has introduced encrypted USB devices for transferring data. These authorised items are available from Emma Todd (PA and Administrator). There are large capacity (750 GB) portable hard drives and smaller 4 GB pen drives for use by staff to move and store all data transferred from PHI systems. With the exception of PHI-supplied laptops/tablets, no other portable media is permitted to be used within the department.

Protect the passwords that protect access to confidential information on portable devices.

PHI approval is to ensure that safety and security features cannot be switched off

3.6 Email

All staff have email and internet access, supplied by PHI via LJMU, and are responsible for the acceptable and appropriate use of these facilities as defined in the Acceptable Use Policy for Internet and Email available at http://www.PHI.org.uk/governance

Internet & Email Acceptable Use summary

- Internet and e-mail users must observe the rules of acceptable use
- Use of the Internet and e-mail facilities for work use is encouraged for the normal execution of an employee's job responsibilities and supports the goals and objectives of the organisation
- Use of the PHI and e-mail facilities for personal use is permitted in accordance with the LJMU policy
- Email is the way all important information is communicated, including warnings and announcements about Health & Safety, IT, staff matters and procedural matters. It is essential that all staff log on to check their emails regularly;
- Consider the effect of using "reply to all" and only include appropriate people. Don't be a "junk-mailer"
- Think calmly and carefully before responding to an email that may be inflammatory, avoid reacting angrily

- Before you “reply to All” or forward email, ensure that you are not sending PID or otherwise sensitive information to unauthorised recipients, by checking lower down the email trail and attachments
- Internet and e-mail use is subject to UK law and PHI policies, and any misuse will be dealt with appropriately
- The use of Internet and e-mail may be monitored from time to time for compliance, security and/or network management reasons, in line with government guidelines, local and national policies
- No member of staff is permitted to transmit, access, display or download offensive or discriminatory material, including hostile text or images relating to gender, ethnicity, race, sex, sexual orientation, religious or political convictions, gambling, disability when using work facilities
- No staff or corporate information may be made available to unauthorised people particularly on Blogging or Social networking websites, either using work facilities or privately. Failure to comply is a breach of Caldicott principles and Data Protection law
- The organisation has the final decision on deciding what constitutes inappropriate use and offensive material, and reserves the right to determine the suitability of use, which if found in breach of the laws or PHI/LJMU policies, may lead to disciplinary proceedings, dismissal and criminal prosecution.

3.6.1 Sending information by email

The organisation email (name@ljmu.ac.uk) has security measures in place for sending information in, or attached to, an email **WITHIN** the organisation (i.e. to another email address in the format (name@ljmu.ac.uk).

It is **NOT SECURE** if you send information from organisation email (name@ljmu.ac.uk) to an email address outside the organisation. This is because when the destination is not in the same domain (name@ljmu.ac.uk), it goes via the internet leaving copies on Internet servers all over the world which are not very secure, allowing hackers to get information that they sell. That includes healthcare information.

If you use an NHS Mail account (email address ending in **nhs.net**) and send an email to another secure email account (another account ending in **nhs.net** or other secure government system), then the system is secure because it is totally encrypted. That’s not just password protected, that means the information is effectively scrambled and cannot be deciphered by hackers.

BUT REMEMBER it is only secure when sending and receiving email addresses are <u>BOTH</u> encrypted accounts, such as NHS.net or any other encrypted email account as used now in many other public organisations, with the following account domains, so sending from nhs.net to one of these is also securely encrypted:

MoD (*.mod.uk)
GSi (*.gsi.gov.uk)
GCSX (*.gcsx.gov.uk)
CJX (*.pnn.police.uk)

GSE (*.gse.gov.uk)
GSX (*.gsx.gov.uk)
CJSM (*cjsm.net)
SCN (*scn.gov.uk

3.6.2 NHS Mail accounts for non-NHS organisations

NHS Mail accounts can be established for organisations outside the NHS, where there are regular communications of PID with them. Contact IT Support for details.

3.7 Moving Forms, Notes and Records to other locations

- Documents containing PID, confidential or sensitive information should be transferred through PHI's Sharepoint secure FTP system.
- If physical movement is unavoidable all papers, electronic storage or other device containing such information must be transported in a secure wallet, pouch, transit-box or other container of appropriate size for the contents, securely closed and marked CONFIDENTIAL, Property of PHI with address to return it to if found
- If you send PID by post internally **DO NOT USE INTERNAL ENVELOPES**, use a normal envelope sealed and clearly addressed because multiple address panels could result in incorrect delivery
- When transferring information in person, the secure containers must be transported securely, out of sight (e.g. in car boot) and not left unattended. Small amounts, even if carried in a briefcase, must still be in a secure container of appropriate size, e.g. secure folders.

3.8 Confidential Waste

Make sure PID is put into Confidential Waste bag or bin, not ordinary waste bins. For waste collection and other estates matters contact Emma Todd.

3.9 Safe Haven Faxing

All Confidential Information, whether it is held on computer or in a manual format, is subject to the Data Protection Act (1998) and all staff are responsible for complying with the Act.

Sending documents by fax when they contain PID, confidential or sensitive information must follow Safe Haven rules to ensure compliance with the law.

Designated Safe Haven fax machines must be located in a secure environment where access is restricted to responsible authorised staff needing access in the performance of their duties.

3.9.1 Safe Haven Fax Procedure summary

- All faxed PID must have a front cover sheet showing source and destination contacts with telephone numbers and number of pages faxed

- Before transmitting PID via fax for the first or only time the recipient's number must be tested, and fax numbers programmed into fax memory to avoid misdialling
- Successful receipt of faxed PID must be verified
- All incoming faxes should be removed from the machine on receipt and be appropriately dealt with
- To transmit PID to a fax that is not a designated Safe Haven carry out this additional procedure **BEFORE** sending it:
    - Inform the recipient that a fax is to be sent, send it then ask the recipient to confirm receipt;
    - Investigate immediately if it goes missing!

4. Information Security Assurance

There are many places where the information we hold is at risk of being disclosed to people who might use it for illegal purposes, or in fact any purpose that the information subject would not want to be associated with.

An individual's information is generally held under legal and ethical obligations of confidentiality. Information provided in confidence must not be used or disclosed in any form that might identify the individual without his or her consent.

All staff must therefore be vigilant when handling personal information so that such risks are minimised and confidentiality is maintained. The most common high risk situations are described in the following paragraphs:

5. Confidentiality

A duty of confidence arises when one person discloses information to another (e.g. individual to medical staff) where they expect that it will be held in confidence. This means they don't disclose any individual or staff information to anyone not entitled to it, as defined in DPA02 Confidentiality Code of Conduct, available at http://www.PHI.org.uk/governance

It is the same when a person gives their information to help with research. It is given on the understanding that it remains confidential.

5.1 Training

All staff must read the DPA Awareness training documentation.
A DPA Awareness training presentation can be found at http://www.PHI.org.uk/governance .

5.1.1 Attending the DPA Awareness and Training presentation

Presentations will be periodically arranged to explain what DPA is all about and why we need to comply.

It doubles as a training session tailored to PHI, with some questions at the end to demonstrate that all staff have a good understanding of the processes to be followed.

All staff are expected to sign a Register to show not only that they have read the documentation, but also to indicate their agreement to comply with all of the Policies & Procedures included.

6. Secondary Use Assurance

6.1 Use of Information

Information that is entered into NHS computer systems may be used for many purposes after a patient has received healthcare, subject to the rules of consent and disclosure.

6.2 Accuracy

Systems are in place to ensure that NHS data accuracy and timing of it is up to the required standard and compares favourably with National levels.

6.3 Data Quality

Data quality across data assets is maintained by applying systems and processes which protect the integrity of the original files and information. Amendments such as the addition of geographic identifiers are made by the IAO using national lookup tables, and labelled explicitly so as to delineate them from the original fields / values.

7. Corporate information management

7.1 Corporate Records

There must be regular auditing of corporate information. All staff must be aware of the information around them – where it comes from, where it goes, who looks after it, how it is stored and how long it is kept. Information Lifecycle Management ensures that we all follow the procedures to manage information correctly.

7.2 Freedom of Information (FOI)

FOI gives everyone the right to ask any public organisation for any information they hold on any subject. Unless there is a good reason not to, the organisation must provide the information within a month and there is a fee for the response.

- Forward all requests you receive for information without delay to the LJMU FOI Lead. If you are unsure if it is an FOI request contact the FOI Lead for guidance
- Maintain and weed your files (electronic and paper) so that they only contain the key decisions/information that you need to refer back to
- Make sure you only keep information for as long as it’s needed or for the required retention periods

- Review your filing practices – all filing should be in a logical and common filing system agreed within your Department, with the approval of the IT Support Manager
- Staff in departments/teams should be able to access each other's filing, storage and retrieval systems in the absence of a member of staff. When an FOI request for information is made it is not acceptable to give staff absence as a reason for not meeting the deadline for response
- Review your documents – all documents should have footers on them that easily identify where they are kept electronically
- Housekeep your PC – we are all much better at saving than deleting – but electronic clutter is just as bad as on paper

Appendix 1 – Confidentiality Summary and Do's & Don'ts

Keeping Confidential Information Secure - Summary

Confidential information must:

- Not be shared or discussed with, or in the presence of, anyone who does not need to know, or is not specifically authorised to know that information
- Have appropriate control applied, having regard to professional ethics and patient consent. Applying formal access controls for clinical records and statutory requirements
- Have appropriate control applied over the disclosure on non-patient information e.g. staff, relative, visitors in accordance with statutory requirements
- Not be shared with parties outside the PHI e.g. solicitors, insurance companies, employers, police without the written consent of the individual concerned unless there are specific powers to do so
- Always be stored in a secure location, preferably a room that is locked and in some cases alarmed when unattended
- Must not in the majority of cases be taken home or removed from PHI without specific authorisation, this specifically applies to patients health records or other sensitive, confidential patient data

For all types of records, staff working in areas where personal records may be seen must:

- Shut/lock doors and cabinets as required
- Adopt a "clear desk" policy where possible
- Wear organisation identification badges or other authorised identification
- Query the status of strangers
- Know who to tell if anything suspicious or worrying is noted
- Not tell unauthorised personnel how the security systems operate
- Not breach security themselves
-

With electronic records, staff must:

- Always log-out of any computer system or application when work on it is finished
- Not leave a PC or terminal unattended and logged-in
- Not share logins with other people. If other staff need to access records, then appropriate access should be organised for them – this must not be by using others' access identities
- Not reveal passwords to, nor ask for the passwords of, others
- Change passwords at regular intervals to prevent anyone else using them

- Avoid using short passwords (use 6-8 characters), or using names or words that are known to be personally associated with them (e.g. children's or pet names or birthdays)
- Use a password-protected screen-saver where possible to prevent casual viewing of patient information by others. Use Ctrl-Alt-Del for this
- Protect information from the view of others as far as possible, taking particular care when there is a visitor present
- Ensure that unwanted confidential printouts are shredded where possible and disposed of in confidential waste sacks and in accordance with Organisation policy on record disposal
- Ensure that electronic media such as floppy discs, CD Rom, USB memory devices and Computer hard drives are disposed of in accordance with Organisation's policies

Staff must ensure that general conversation involving discussions about individuals (including telephone) wherever possible is:

- Undertaken in an area out of earshot of others, preferably in a closed office
- Not undertaken with anyone who is not authorised to receive the information, including family and friends of the subject

Confidential information sent via internal post or in internal transit must always be:

- Appropriately addressed to a named recipient, post holder, consultant or legitimate Safe Haven (Organisation nominated secure area)
- Sealed in an appropriately secure envelope/package (not with multiple address panels) based on sensitivity and volume
- Marked accordingly, with "Confidential" or "Addressee Only" as appropriate
- Traced in or out and signed for as appropriate

Confidential information sent via external post or in external transit must always:

- Be addressed fully and marked accordingly, with "Confidential" or "Addressee Only" as appropriate
- Be sealed in an appropriately secure envelope/package based on sensitivity and volume and using tamper proof seals where practicable and appropriate
- Be sent via an approved carrier such as courier, Internal post or special delivery for any confidential information sent, obtaining a receipt as proof of sending/delivery is advised where possible
- Traced in or out and signed for as appropriate

Staff wishing to send or receive confidential information via fax must:

- Follow the PHI Safe Haven fax Procedures in Section 9 of DPA02

Confidentiality Code of Conduct which can be found at http://www.PHI.org.uk/governance

- Use a cover sheet
- Only send personal identifiable data to a recognised Safe Haven (nominate secure area) fax number
- Address the fax to a named recipient
- Always check the number to avoid misdialling, check the number is correct and current if stored in a fax memory prior to sending
- Ensure that organisation fax machines are placed in secure locations, preferably within the boundary of a Safe Haven (organisation nominated secure area). As a minimum fax machines should be locked when unattended, switched off outside normal working hours or safely secured in lock cupboards if left switched on

Staff using E-Mail must:

- Not e-mail patient identifiable information externally to PHI unless standard encryption software has been implemented and approved by IT Support, or unless using NHSMail to NHSMail (or other government approved secure email system)
- Unless you have been formally advised of the encryption implemented no data may be sent
- Only e-mail person identifiable information when the DPA Principles are applied (anonymised where appropriate and the minimum identifiable data necessary)
- Apply adequate protection by placing the information in a password protected attachment where possible (internal use only)
- Check to ensure that the recipient is authorised to receive the data (be careful of shared mailboxes)
- Ensure that extra care is taken to ensure that it is sent to the correct person (use of personal address books is recommended)

The Top Ten DPA Things To Remember

1. Follow the Data Protection Principles
2. Respect Confidentiality of individual and staff information
3. Obtain consent to use someone's personal, sensitive, confidential information
4. Understand when you are obliged to disclose information
5. If someone asks to see their Staff information direct them to HR at LJMU
6. If someone wants information about the PHI or LJMU, direct them to the FOI Lead
7. Don't share your password
8. Keep information safe, transfer sensitive information in secure containers
9. Report breaches of Confidentiality or Security
10. **When in doubt, ask for advice**