

COMMISSIONING PCT Information Security Staff Policy 2011 – 2013

Approval Process

Lead Author: ASP Change & Information Security Manager

Reviewed by: Information Governance and IM&T Group

Approved by: NHS Cambridgeshire and NHS
Peterborough Information Governance
and IM&T Group and NHS Peterborough
Information Governance Steering Group

Ratified by: Governance and Compliance Committee

Date ratified: February 2011

Version: 1.1

Review date: April 2013

Valid on: February 2011

Signatures for Ratification

1. Name Title

Signature Date

2. Name Title

Signature Date

Document Control Sheet

Development and Consultation:	This is a new policy that replaces the Information Security Policy v3.0 and the IT Security and Usage Policy v3.0. It was developed by the ASP Change and Information Manager in consultation with ASP partner organisations Information Governance and IM&T Groups and endorsed by the Governance and Compliance Committee and PCT Boards.
Dissemination	This policy will be promoted within the Commissioning PCTs and uploaded to the website
Implementation	The Director of Corporate Development and Performance (SIRO) is responsible for monitoring the application of the policy by ensuring that: - <ul style="list-style-type: none"> • The policy is brought to the attention of all employees • Managers are aware of their responsibilities for ensuring that staff under their control implement the policy • Appropriate training and guidance is provided to staff • Corporate business processes support the implementation of the policy • Security is everyone's responsibility
Training	Training will be undertaken as part of the PCT's ongoing processes.
Audit	Implementation of the Policy will be monitored on a regular basis and in conjunction with the PCT's Information Governance Toolkit requirements 301, 302, 305, 310, 313, 314, 323 and 324 at level 3.
Review	This policy will be reviewed bi-annually, or earlier if there are changes in procedures or legislation.
Links with other DtGP	The Policy should be read in conjunction with: Information Governance Policy, Code of Conduct for Confidentiality, Email Acceptable Use Policy, Home Working Policy, Records Management Policy, Internet Acceptable Use Policy, Removable Media Policy, Safe Haven Policy, Destruction and Disposal of Unwanted Information and Equipment Policy, Registration Authority Smartcard Policy, Records Preservation, Retention & Destruction Policy, Data Protection & Access to Records Policy, Cambridgeshire NHS & Health & Social Care General Protocol for protecting and Using Personal Information within Cambridgeshire & Peterborough
Equality and Diversity	The Information Governance team have carried out a Rapid Equality & Diversity Impact assessment and concluded the policy is compliant with the PCT Equality and Diversity Policy. A few negative impacts were identified but none required action

Revisions

Version	Page/ Para No	Description of change	Date approved
1		ASP re-write of previous policy	February 2011
1.1	Page 8 Page 9 Page 16 Page 23	Change to reflect local process for authorisation of encrypted USB sticks and clarity re screensavers Section 6, changed to 7. Word 'must' replaced with 'will' Additional guidance documents added	May 2011

1.2	Title Page Page 8 Pages 11 Page 12	Joint NHSC & NHSP Logo added Removed NHSC in front of Removable Media Policy Data storage F:\ added Data storage K:\ added	Dec 2011
-----	---	--	----------

CONTENTS

1.	Purpose and Scope	page 4
2.	Background	page 4
3.	Duties and Responsibilities	page 5
4.	Data Security	page 5
5.	Network Security	page 8
6.	Computer Security	page 11
7.	Virus Control	page 15
8.	Email	page 17
9.	Internet	page 20
10.	Security Incident Management	page 21
11.	Non-compliance	page 22
12.	Statutory and other relevant guidance	page 22

1. PURPOSE AND SCOPE

This policy covers the security and use of information technology and applies to ASP, their partners and all organisations (hereafter referred to as organisation(s)) to whom ASP provide ICT services. These organisations include:

- Anglia Support Partnership
- Cambridgeshire and Peterborough NHS Foundation Trust
- NHS Cambridgeshire
- Cambridgeshire Community Services NHS Trust
- NHS Peterborough
- Peterborough Community Services
- East of England Strategic Health Authority
- Health Protection Agency

This policy also applies, where appropriate, to staff from other organisations who log in to ASP managed computers initially, but then obtain applications from their host organisation e.g. via remote services.

The purpose of the security policy is to help protect the organisations from hazards and threats, and to ensure that the valuable information held in information systems is secure from accidental or deliberate unauthorised modification or disclosure.

2. BACKGROUND

The organisations' communications and computer systems are provided for business use and are to be operated and used accordingly.

Use of the organisations' computer systems are based on the following principles and this policy states your responsibilities to abide by them:

Confidentiality Access to information should be restricted to people who need to see it and are allowed to see it.

Integrity Is the requirement to ensure that all system assets are operating correctly according to specification and therefore showing you the information as it was entered onto the system.

Availability Is the requirement to ensure that information is delivered to the right person, in the right place, at the right time i.e. when and where it is needed.

This policy has been written to be unbiased, and does not discriminate regarding age, sex, disability, race, religion or similar belief with regard to the security and confidentiality issues it covers.

3 Duties and responsibilities

The overall responsibility for maintaining and implementing the organisations' information security policy lies with that organisation's chief executive.

Senior Information Risk Owner (SIRO) is responsible for leading on the risk management of information security within the organisation.

The Information Governance and IM&T Steering Group and the Head of IT are responsible for promoting Information Security within the organisation and providing guidance and advice.

Directors are responsible for ensuring that this Policy is implemented within their individual Directorates and ensure ongoing compliance.

All staff have a duty to comply with the policy and to report any information security incident or risk to the relevant member of staff as outlined within the policy.

4 Data Security

4.1 Patient Identifiable Data (PID)

What is PID?

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, address
- Full post code
- 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.

Sharing patient information

Patient identifiable data must not be shared with people who are not authorised to see it. Only those staff, which as a result of their tasks require access to patient identifiable data, should be allowed to access such data. Whenever possible patient data should be anonymised.

Identifiable patient information

The number and type of health and social care related data items, which could allow identification of an individual, should be reduced to the minimum essential for the purpose if not anonymised.

Access limitations principles

There should be locally agreed arrangements for ensuring that patients are personally made aware of the purposes to which information about them may be put, as well as ways in which they can exercise choice.

4.2 Personnel Data

Personnel files also contain personally identifiable data and must be kept in accordance with the Data Protection Act. It is the Manager's responsibility to ensure that electronic and paper records are securely saved/stored. This information must be stored in a locked filing cabinet with controlled and limited available access to this sensitive data. Personally identifiable data must not be shared with individuals other than when strictly necessary, or left unattended, such as on a desk.

4.3 Business Confidential Data

What is Business Confidential Data?

In general terms, business confidential data includes any information that is not available to the public. Data that is highly confidential is information, which would damage the organisations' business if it became known to a wider public base.

Confidential data is one of the partners' most valuable assets. If that information becomes public, it may affect the organisations' competitiveness and put at risk the livelihoods of you and all of your colleagues.

4.4 Exchanging Patient/Person Identifiable & Business Confidential Data

Exchange of data between organisations must be controlled.

The only secure method of exchanging data by email is to use NHS Mail (@nhs.net) i.e. both sender and recipient must use NHS Mail accounts. For more information see the Email Acceptable Use Policy.

Due to the large number of staff in the NHS Mail address list, extreme care must be taken to ensure that your email is addressed to the intended recipient.

If NHS Mail is not available to both parties then an alternative method of transmitting/transporting the data will need to be used and the files must be encrypted.

NB. Microsoft Office applications have the facility to password protect files – this is not encryption. These passwords can be broken and therefore this should not be considered as a safe means of protecting the data.

Removable Media

If files are copied to floppy disks or CD/DVDs (for exchange between organisations) then they must be encrypted. For help and advice on encryption methods contact the ASP ICT Service Desk.

Only encrypted USB memory sticks are approved for the use of transporting data files. Encrypted USB memory sticks are available through the completion of forms contained in the Removable Media Policy. Please check with your Information Governance (IG) department if further information is required.

When no longer required, removable media (encrypted or otherwise) must be securely disposed of. Removable hard disk drives and USB memory sticks must be returned to the ICT department for secure disposal. Please check with your IG department for any local arrangements for disposing of CDs, DVDs and floppy disks.

Encryption Standards

When data is transmitted e.g. via email, the level of encryption used must meet the minimum standards as defined by NHS Connecting for Health. If you have a business requirement to encrypt data, and require assistance please contact the ASP ICT Service Desk.

Security of data in transit

If copies of data need to be transported between sites on physical media, then organisationally approved secure couriers must be used.

A secure courier is not an internal post service or member of staff who happens to be visiting a location for some other purpose. A secure courier will be able to provide adequate security assurances (set out in a written contract) and a tracked mode of collection and delivery.

Security of data when faxing

The transmission of confidential data (whether patient, personnel or business) by fax must be carried out in accordance with your own organisation's Safe Haven Policy.

NB. Some older fax machines are fitted with a ribbon type cartridge. The ribbons in these cartridges hold an imprint of the data that has been printed on the fax machine, and therefore must be disposed of securely.

4.5 Security of data when printing

If you need to print documents that contain patient/person identifiable data, then it is your responsibility to ensure you are sending the document to the correct

printer. If you have the option to use a 'secure print' function it is best practice to do so.

Printed documents of this nature must be accompanied by a header sheet clearly identifying who the print belongs to, and how to contact them.

Printed documents of this nature must be collected from the printer immediately and not left unattended.

If you discover a document containing patient/person identifiable data on your printer which has not been collected by the rightful owner, please take the following action:

- Notify the owner immediately.
- If it is not practical for the owner to securely collect the document it must be shredded.
- Retain the header sheet.
- Report the incident to your Information Governance/Information Security Manager.

5 Network Security

5.1 System Access Control

System access must be authorised by your line manager or the appropriate Information Asset Owner (IAO).

Managers and IAOs must send all starter, amendment & leaver system access requests to the ASP ICT Service Desk via email, using the appropriate form (where available) for the system access being requested. These requests will not be accepted via telephone, fax or post.

System privileges and access rights will be allocated on the basis of your specific role requirements; they are not based on the status of your role.

System usernames and passwords that are allocated to you, are your responsibility and for your use only.

Never share your system access account with anyone else. If someone else logs in as you, whatever they do will be registered against your name.

Never use someone else's system access account.

Ensure that PCs/terminals are logged off when left unattended or lock the screen by invoking the screen saver using the **CTRL-ALT-DELETE** keys and select '**Lock Computer**'. Screen saver is automatically generated when terminals are 'idle' for more than 5 minutes.

All detected unauthorised attempts at system access must be notified to the ASP ICT Service Desk. ASP will notify all incidents to your organisation's IT

management for investigation. Your organisation's IT Management must ensure that the organisation's IG lead is informed to facilitate any required investigation.

5.2 Password Security

Password Security is the responsibility of the individual. You remain accountable if you give your password out for system activity under your username. Giving your password out lets others assume your identity. They can send email in your name, access your personal files or even add false information to patient records.

Never share your password with anyone else.

Never write your password down.

For security reasons, most systems will require you to change your password periodically. However if you feel your password may be compromised, do not wait until the system asks you to change it, do so immediately.

When allocated a new password (either when your account is first issued to you or following a change of password at a later date) most systems will immediately require you to change it. If the system does not force a password change immediately, then manually change the password as soon as possible. Do not continue to use the password that has been allocated to you.

Passwords should be formulated in such a way that they are easily remembered but difficult to guess. Passwords should not relate to the system or the user e.g. do not use well known family or pet names. A balance between usability and security is best.

Passwords must consist of a minimum of 8 characters, but for improved security they should include upper and lower case letters, plus numeric and/or special characters where the system allows.

In exceptional circumstances, where authorised by your organisation, generic accounts may be set up for specific purposes. These account details must only be shared with authorised members of staff, and the password must not be written down for all to see e.g. on a post-it note, taped to the base of removable media etc.

If access to another user's mailbox or personal drive is required in circumstances where absence from work is unexpected e.g. sick leave, personal emergencies etc. and there is an immediate business need to have access to this information, then this access must be authorised by the employees Director. Please see the "Procedure for gaining access to another individual's mailbox or personal drive" which is available on the ASP Extranet.

5.3 Account/Password Sharing

If it is discovered that a member of staff is sharing their account and password details, the account(s) in question will be disabled.

The incident will be reported to the organisation's Information Governance Manager (or equivalent).

The account will only be re-enabled when authorisation to do so is received via email from the relevant organisation's Information Governance Manager (or another member of senior management).

Sharing passwords, and logging onto the network as another individual is a breach of this policy and may lead to disciplinary action being taken against you. (See section 11 Non-Compliance).

5.4 SMART Card Security

SMART cards are issued to staff to provide access to NHS national applications. Through SMART card access individuals are enabled to access personally identifiable patient or personnel data which is extremely sensitive and confidential in its nature.

They are issued on an individual basis and remain the responsibility of that individual.

Never share your SMART card or PIN with anyone.

Never allow another member of staff to use the system while you are logged in with your SMART card.

Never use the system while someone else is logged in with their SMART card.

Never write your PIN down nor stick it to your SMART card.

Never leave your SMART card in the card reader when it is not in use.

Always store your SMART card in a secure place – do NOT leave it lying around.

If your SMART card is lost or stolen report it to your line manager and the ASP ICT Service Desk immediately.

Where national applications have Role Based Access Controls (RBAC), legitimate relationships are created through RBAC and patient consent. Your organisation will receive reports detailing user access to records where there is no apparent legitimate reason to do so. These reports will be investigated by your organisation to establish if the access was appropriate. Inappropriate access may result in disciplinary action.

5.5 Data Storage

Various network drives are provided to enable staff to store data securely. The data on these drives is backed up on a daily basis.

Personal Drive

Your personal drive e.g. P:\ or F:\ is provided to enable you to save work related files that pertain only to yourself e.g. HR or appraisal related documents. This area is not provided for storing personal data e.g. photographs of family and friends, music files etc.

Shared Drive

The shared drive e.g. S:\ or K:\ is where any non-confidential work related files should be saved. This area should contain files which it would be appropriate to share across departments or directorates.

Restricted Drive

The restricted drive e.g. R:\ is for saving any confidential work related files. This will contain files that should only be seen by a limited number of staff e.g. within a small team, a manager & PA etc., and where it would not be appropriate to save them on the Shared drive

Local Drive

In some circumstances staff may have access to their local drive e.g. C:\.

NEVER save data on the local drive as it is not secure. This drive is not backed up by the ICT department so if files were lost or corrupt ICT will not be able to retrieve them.

If the computer were lost or stolen, the security of any data saved on the local drive will be compromised.

6 Computer Security

6.1 Software

All software must be approved by your organisation, prior to purchase, and appropriately licensed. The use of unlicensed software is prohibited.

New software, not previously used by your organisation, must be approved:

- By your organisation's IT lead e.g. to assess business need, cost, privacy impact etc.
- By ASP's Change Management process e.g. to assess network security, network performance impact, additional technical requirements etc.

Staff are not authorised to install any software to their work computer – whether desktop or mobile device. This includes software downloaded from the Internet as well as software on physical media.

All software must be installed by ASP ICT staff to ensure licensing is legal. If you require additional licensed software to be loaded please contact the ASP ICT Service Desk.

Software must also be removed by ASP ICT staff, to ensure that it is uninstalled correctly, and to enable licensing records to be maintained. If you require software uninstalling please contact the ASP ICT Service Desk.

Non-NHS procured software will not be installed onto an organisation's computer equipment.

Software obtained illegally will not be installed onto an organisation's computer equipment.

Any and all instances of unauthorised installations of software will be reported to the staff member's organisation.

6.2 Hardware

All computer equipment must be authorised by your organisation and procured through the ASP Purchasing Department. Non-NHS procured and/or personal computer equipment must not be connected to the organisation's network. Non-NHS procured and/or personal computer equipment will not be supported by Anglia Support Partnership.

Any and all instances of personal devices connected to the partner network will be reported to the staff member's organisation.

The organisation's computers are provided as tools for you to do your job; they do not act as a personal computer. They are subject to security controls and they cannot be treated in the same way as your PC at home.

6.3 Physical

Ensure that your computer and related media are physically secure.

Keep technology out of public view where possible; use blinds, keep doors closed etc. Lock office doors when computers are left unattended.

Keep removable media - CDs, floppy disks, USB memory sticks – locked out of sight.

Where computers are used in public areas, make sure the screen cannot be viewed by members of the public, except where this is a requirement for this e.g. touch screens for patient use.

All members of the ICT department are issued with ID cards and must carry them at all times. Do ask them to produce their ID card if you are unsure as to their identity, before you allow them to access or remove your computer.

6.4 Modems, faxes and the NHS Code of Connection

Connecting computer equipment directly to the Internet or a telephone line (e.g. via broadband or a 3G modem) while simultaneously connecting it to the NHS Network (e.g. via network cable at an NHS site), contravenes the NHS Code of Connection.

Computer equipment includes:

- Desktop computers
- Laptop computers
- Multi function devices (MFD) i.e. fax/printer/photocopier/scanners
- Network infrastructure

Modems include:

- Dial-up modems
- Broadband modems/routers
- 3G wireless modems

Some examples which would constitute a breach would be:

- A laptop connected to the ASP managed network via cable while simultaneously connected to the Internet via a 3G modem card.
- An MFD connected to the network via cable (to be used as a network printer) while simultaneously connected to a phone line as a fax.

6.5 Mobile Computing

This section covers:

- Portable Computers (Laptop and Notebook computers)
- PDAs
- Palmtops
- Advanced Mobile Phones including Blackberry devices
- Remote Access (RAS) / VPN Tokens

Only mobile computers authorised by your organisation and procured through the ASP Purchasing Department must be used by staff. Personal mobile computers must not be used for business purposes, nor connected to the NHS network.

The only exception whereby personal computers can be used for business purposes is when you have been authorised to use the 'work from home/secure desktop' solution. To maintain security, this solution can only be used in conjunction with an ASP VPN token

Synchronisation will only be supported between an ASP procured mobile device and the member of staff's NHS email account.

All mobile computers must have their storage drives encrypted. If yours is not, or you are not sure that it is, please contact the ASP ICT Service Desk.

Never save person identifiable data (PID) on your mobile computer e.g. the C:\ drive of your laptop.

Mobile computer security is your responsibility at all times.

Mobile computer devices must be password protected.

If you have and use a portable computer security cable, keep one key with you and the other in a secure separate location.

Never leave the mobile computer unattended in a public place.

The mobile computer must be securely locked away when not in use.

Ideally mobile computers should not be left in your car. However, if doing so is unavoidable, never leave the mobile computer in view in the inside of your car - lock it away in your car boot.

Portable computers (e.g. laptops and notebooks) need to receive updates e.g. anti-virus and Windows updates, on a very regular basis. To facilitate this, your computer needs to be connected either to the organisation's network or the Internet (via your broadband connection at home) frequently. Please see Section 7 – Virus Control for further information.

Never leave your VPN token or smart card in the same location as the mobile computer.

Avoid leaving the mobile computer within sight of ground floor windows or within easy access of external doors.

Never write down passwords and store them with the mobile computer.

Damaged or broken mobile computer devices must be returned to the ASP ICT department before being sent for repair, to ensure that the device is re-imaged/erased by an ASP ICT engineer and any data is removed. If the device cannot be repaired then it will be disposed of in accordance with the Disposal of IT Equipment policy and WEEE regulations.

All mobile computer devices must be returned to your manager if they are no longer required e.g. following a change of post, leaving the organisation etc.

6.6 Remote Access (RAS) / VPN Tokens

VPN tokens are issued to staff to allow secure connection to N3 (the NHS network) and/or the ASP partner network when working remotely e.g. from home.

These tokens represent a significant security risk to the NHS & partner organisation's networks and therefore patient information, should they be lost or stolen. Therefore these tokens must be stored securely at all times. They must not be stored with the laptop computer that they are configured to be used with (so as to minimise the risk of both items being lost or stolen together).

The username and password/PIN must never be written down nor stuck to either the VPN token or the laptop.

All VPN tokens must be returned to your manager if no longer required.

If a VPN token is lost or stolen, it must be reported immediately to the ASP ICT Service Desk.

6.7 Working From Home

For information on working from home please refer to your own organisation's Home Working Policy where available.

7 Virus Control

All computers (laptop and desktop) must have an anti-virus software package installed. Staff are not allowed to alter the configuration of this package. If you feel the configuration of the anti-virus software needs amending please contact the ASP ICT Service Desk.

Anti-virus software has been installed to prevent an attack from malicious software and to prevent loss of data and corruption of programs/files.

Anti-virus software needs to be updated on a very regular basis. To facilitate this, your computer needs to be connected either to the organisation's network or the Internet e.g. via your Broadband connection while using your laptop from home. Laptops must be connected, at the least, on a monthly basis, to ensure anti-virus is kept up to date.

Windows updates are also essential to protect your computer, however laptops will only receive these updates when connected directly (i.e. not using your VPN token) to the organisation's network. Therefore you must return your laptop to your place of work and connect it to the network on a regular basis – at the very least quarterly. The more frequently you do so, the less time it will take for the updates to be applied.

If your computer's anti-virus software is not updating automatically please contact the ASP ICT Service Desk immediately.

All virus infections must be reported to the ASP ICT Service Desk as soon as possible.

If a virus is discovered the following actions must be carried out:

- Turn the computer off immediately (using the power button if you are unable to control the PC and shut it down in the usual manner) OR disconnect the network cable – whichever is quickest.
- Inform the ASP Service Desk.
- Place a label over the power button stating that the machine has a virus infection and must not be used.
- Isolate any floppy disks and USB memory sticks (external storage) that have been used on that computer.

7.1 Viruses with Email messages

Although the organisations' email system runs up to date anti-virus software, it is not guaranteed that all viruses will be stopped. It is therefore important that e-mails, especially those that have attachments or contain Internet links, from unrecognised sources are regarded with suspicion as these are common ways of distributing viruses.

However, although it makes sense to be cautious about email attachments from people you don't know, that does not guarantee that attachments from someone you do know will be safe. Worm type viruses generally spread by sending themselves without the knowledge of the person whose account they spread from.

Caution is recommended at all times - even a legitimate, expected attachment could be virus infected.

The following are some examples of emails which should be regarded with particular suspicion:

- Emails that come from someone you do not know who has no legitimate reason to send them to you.
- An email that does not have any message but contains an attachment.
- An email that contains some text in the message, but it does not mention the attachment.
- An email that contains a message, but it does not seem to make sense.
- An email that contains a message, but it seems uncharacteristic of the sender.
- Any email containing unusual material e.g. pornographic web sites, erotic pictures etc.

- Any email that contains a short, non-business related statement e.g. "You must take a look at this", whether in the subject line or the body of the message.
- If the attachment has a filename with a "double extension", like FILENAME.JPG.vbs or FILENAME.TXT.scr, this would be extremely suspicious. As far as Windows is concerned, it is the last file extension that determines the type of file.

The email system will remove many types of attachment that are of a high risk nature e.g. when the file extension indicates it is an executable programme, or a compressed (zipped) file.

Encrypted files can contain any kind of file and cannot be scanned by anti-virus software. Consequently, the computer system's anti-virus software will remove encrypted files that are attached to emails for safety reasons.

If you have a business need to send or receive compressed and/or encrypted files please contact the ASP ICT Service Desk.

However, even files that the email system does allow e.g. Microsoft Office attachments, are not guaranteed to be safe. There are filenames like .rtf that shouldn't include program content, but sometimes can, therefore caution needs to be exercised at all times.

If you are in any doubt whatsoever as to the validity of the email or attachment, check with the sender as to whether or not they knowingly sent the mail/attachment in question. If they did not, please contact the ASP ICT Service Desk immediately.

Avoid Unnecessary Macros

If Word or Excel warns you that a document you're in the process of opening contains macros, regard the document with particular suspicion unless you know that it's supposed to contain macros. Even then, don't enable macros if you don't need to. Check with the person who sent it to you that it is supposed to contain macros.

8 Email

It is recognised that email is a useful means of communication, a valuable resource and essential to support NHS business. Email enables employees to communicate promptly and efficiently with other employees, teams, individuals and organisations and for them to undertake their role efficiently and effectively.

Email is primarily for business use. Employees are permitted to use email for occasional and reasonable personal use, subject to the terms outlined in your organisation's Email Acceptable Use Policy.

8.1 Monitoring

All employees need to be aware that the employing organisation can monitor the use of email facilities for the following reasons:

1. To ensure compliance to this policy.
2. To protect the organisation from a host of legal liabilities including harassment and discrimination in the work place, defamation, transmitting of confidential information.
3. To guard against inappropriate and excessive personal use.

For further information please see the Email Acceptable Use Policy.

8.2 Disclaimers

The use of email disclaimers are recognised as good practice, but are not legally binding. Should you wish to use an email disclaimer please follow your own organisations' guidelines on style and wording. Anglia Support Partnership staff must use the Auto Signature Template in the ASP House Style section of the ASP Extranet.

8.3 Harassment

What is harassment?

All employees must be allowed to work in an environment free from harassment of any kind. This includes (but is not limited to) sexual and racial harassment, and harassment on the grounds of sexual orientation, religion, age and disability. Harassment affects morale and prevents a person fulfilling their full potential in their work.

Sexual harassment is unwanted conduct of a sexual nature, or other conduct based on sex affecting the dignity of women and men at work. In the context of this Policy this includes sending messages with sexually suggestive material, repeated offensive sexual propositions or abuse of a sexual nature.

Racial harassment is unwanted conduct based on race affecting the dignity of women and men at work. In the context of this Policy this includes sending messages containing offensive insults or "jokes" based on race and abuse of a racial nature.

What you must not do:

Do not send, forward or redirect abusive or offensive messages or messages which contain sexual or racist material.

What are the consequences of not following this policy?

Harassment is a criminal offence for which the harasser can be found personally liable. Victims of harassment may be able to claim damages from the harasser and from the organisation.

Failure to follow these rules may lead to disciplinary action being taken against you. (See section 11 Non-Compliance.)

Reporting harassment:

Any employee who is subjected to or has knowledge of harassment (whether emanating from inside or outside of the organisation) is encouraged to immediately report that harassment to:

- a. The victim's or the witnesses' manager or, where that is not possible or appropriate;
- b. Any member of management at the same level of management as the victim's or the witnesses' manager or, where that is not possible or appropriate;
- c. To any member of the next level of management above the victim's or the witnesses' manager.
- d. To your organisation's Human Resources department.

8.4 Defamation

What is defamation?

Defamation is the publication of a statement that adversely affects a person's, or the organisation's reputation. Publication may be by way of the Internet or via email.

What you must not do:

Do not send or circulate, internally or externally, any information, which is defamatory. In particular, you must not send or circulate, internally or externally, any information that contains negative comments about an individual or company without first checking that the contents of the information are accurate. If in doubt, you must check with your manager.

What are the consequences of not following this policy?

A person or company defamed may sue you and the organisation for damages. There is a defence that the information was "true" but the onus would be on you or the organisation to show that.

Failure to follow these rules may lead to disciplinary action being taken against you. (See section 11 Non-Compliance.)

8.5 Contracts

A contract is an agreement between two or more parties to create legal obligations between them.

Anglia Support Partnership's Purchasing Department provides a centralised, electronic ordering service. ASP Purchasing Department follows all current legislation and the financial standing orders for the organisations for which they undertake to carry out the tendering process.

Please contact ASP Purchasing when you wish to contract with suppliers.

Contracts must not be negotiated via email.

9 Internet

It is recognised that access to the Internet is a useful means of communication, a valuable resource and essential to support NHS business.

The Internet is primarily for business use. Employees are permitted to use the Internet for occasional and reasonable personal use, subject to the terms outlined in your organisation's Internet Acceptable Use Policy.

Occasional and reasonable personal use of the Internet is a benefit and not an entitlement. This benefit may be withdrawn at anytime, for either a specific individual or for all employees of the organisation. Employees will be informed prior to access being revoked.

For further information please see the Internet Acceptable Use Policy.

9.1 Social Networking & Blogging

Social networking sites (e.g. Facebook, MySpace) allow users to create a representation of themselves (a profile), which contains information such as their interests, photographs, social links etc. They allow users to interact over the Internet.

Blogging sites are a type of website, usually maintained by an individual, with regular entries of commentary, descriptions of events, or other material such as graphics or video clips.

These sites must not be used to hold or comment on business related information of any kind.

These are regarded as a personal pastime and consequently they are blocked by the Internet filter, as excess usage could have a detrimental impact on the ASP partner network.

If you have a genuine business need to access such sites, please in the first instance discuss this with your manager. If they feel your request is valid they can contact the ASP ICT Service Desk for a Web Filter Change Request form.

9.2 Streaming Media

Streaming media i.e. video clips (e.g. YouTube) which are available on many Internet websites can use a considerable amount of network bandwidth. Consequently this has been blocked by the Internet filter to protect system performance.

If you have a genuine business need to access streaming media on specific sites please in the first instance discuss this with your manager. If they feel your request is valid they can contact the ASP ICT Service Desk for a Web Filter Change Request form.

9.3 Sexually Explicit Material

The vast majority of staff will not have any legitimate business use for accessing or transmitting sexually explicit material at work.

In exceptional circumstances there may be clinical reason to access sexually explicit material. In such rare occasions prior approval must be obtained from your Director.

What you must not do:

Do not access or transmit any material with a sexual content.

What are the consequences of not following this policy?

Accessing and transmitting sexual material may be a criminal offence for which both you and the organisation could be liable.

The display on screen of sexual material or the transmitting of such material to other people may constitute sexual harassment (see the harassment section of this Policy).

Failure to abide by this policy may lead to disciplinary action being taken against you. (See section 11 Non-Compliance.)

10 Security Incident Management

All incidents that constitute a loss of hardware or data, which could potentially lead to a breach of confidentiality (whether patient, personnel or business), must be reported to your organisation's Information Governance Manager and to the ASP ICT Service Desk.

The organisation's Information Governance Manager will instigate investigation procedures to try and establish the nature and potential threat of the incident and advise the organisation on recommended action.

Incidents could involve:

- Theft or loss of hardware
- Theft or loss of software or data
- Unauthorised or malicious alteration of data
- Unauthorised system access
- Password sharing
- Misuse of system/privileges
- Illegal software download
- Virus attack

All information security incidents are to be recorded on Datix (ASP's Risk Reporting system) via the ASP Extranet.

11 Non-Compliance

Any breach of this policy can result in disciplinary action being taken against you, up to and including your dismissal, according to your organisation's disciplinary policy.

Non-compliance can also damage the reputation of the organisation and open the organisation and individual to a host of legal liabilities.

If further clarification is required please, in the first instance, contact your manager. For further advice and assistance contact your own organisations Information Governance Manager and/or Human Resources Department.

12 Statutory and Other Relevant Guidance

All users of the organisations' computers have a responsibility to abide by the following legislation:

Legislation	Notes
Copyright, Designs and Patents Act (1988)	This Act is the statutory basis of copyright law (including performing rights) in the United Kingdom.
Access to Medical Reports Act (1988)	An Act to establish a right of access by individuals to reports relating to themselves provided by medical practitioners for employment or insurance purposes and to make provision for related matters
Access to Health Records Act (1990)	Majority of this Act repealed by Data Protection Act 1998. Now covers access to deceased patient records only.
The Computer Misuse Act (1990)	This act makes it a crime to gain

	unauthorised access to computers.
EU Data Protection Directive (EU Directive 95/46/EC) (1995)	Concerning the protection of individuals with regard to the processing of personal data and on the free movement of such data.
Protection From Harassment Act (1997)	An Act to make provision for protecting persons from harassment and similar conduct.
The Data Protection Act (1998)	Defines UK law on the processing of data on identifiable living people. An Act to establish a right of access to health and social care records by the individuals to whom they relate and other persons; to provide for the correction of inaccurate health records and for the avoidance of certain contractual obligations; and for connected purposes.
The Freedom of Information Act (2000)	This act creates a general right of access, on request, to information held by public authorities.
Regulation of Investigatory Powers Act (2000)	This act deals with interception of communications, surveillance, decryption of intercepted material and the investigatory & intelligence services.
Waste Electrical and Electronic Equipment Regulations (2006)	These regulations aim to reduce the environmental impact caused by the disposal of electrical equipment.

Relevant Guidance

Fax Printer Ribbon and Film, Department of Health Informatics Directorate, January 2011

<http://www.connectingforhealth.nhs.uk/systemsandservices/infogov/links/ribbons.pdf>

Maintenance and Secure Disposal of Digital Printers, Copiers and Multi Function Devices, Department of Health Informatics Directorate, July 2010

<http://www.connectingforhealth.nhs.uk/systemsandservices/infogov/links/multifuncdev.pdf>

12.1 Copyright

What is copyright?

The owner of copyright has the exclusive right in certain works such as documents, articles, books, plays and musical compositions, so that they cannot be copied or used in certain other ways without the consent of the copyright owner.

What you must not do:

No copyright material should be copied without the copyright owner's consent.

Do not download, copy or transmit to third parties the works of others without their permission as this may infringe copyright. Copyright is most likely to be breached:

- a. when you download material from the Internet
- b. when you copy text or attach it to an email message.

What are the consequences of not following this policy?

You and the organisation can be sued by the owner of the copyright for damages for unauthorised use of the copyright material.

12.2 EU Data Protection Directive

The EU directive "For the protection of individuals with regard to the processing of personal data and the free movement of such data" was adopted in July 1995.

The scope of that directive includes manual as well as automatically processed personal data. Additionally, all staff fall under a common law obligation to preserve the confidentiality of this information.

12.3 The Data Protection Act

The Data Protection Act 1998 became effective from 1 March 2000, and superseded the Data Protection Act 1984 and the Access to Health Records Act 1990. The Data Protection Act 1998 gives every living person the right to apply for access to his or her health and social care records. The exception to this is the records of deceased persons, which are still governed by the Access to Health Records Act 1990.

The Eight Data Protection Principles as laid down in the 1998 Data Protection Act must be followed at all times:

1. Data must be processed fairly and lawfully.
2. Personal data shall be obtained only for one or more specific and lawful purposes.
3. Personal data shall be adequate, relevant and not excessive in relation to the purpose(s) for which they are processed.
4. Personal data shall be accurate and where necessary kept up to date.
5. Personal data processed for any purpose(s) shall not be kept for longer than is necessary for that purpose.
6. Personal data shall be processed in accordance with the rights of data subjects under the 1998 Data Protection Act.

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.
8. Personal data shall not be transferred to a country 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.

12.4 Caldicott Guardians & The Data Protection Act

The 1998 Data Protection Act is the key legislation covering all aspects of information processing. This includes security and confidentiality of personal information. The Caldicott requirements provide the framework to put the Data Protection Act into operation.

The Caldicott Report recommends that a senior health professional in each Health Authority, Trust and other Primary Healthcare Provider, be nominated as the Caldicott Guardian of clinical person identifiable information.

All employees, as laid down by the NHS Executive, must also follow the six Caldicott Principles:

1. **Justify the purpose(s)**
Every proposed use or transfer of patient identifiable information within or from an organisation should be clearly defined and scrutinised, with continuing uses regularly reviewed by an appropriate guardian.
2. **Do not use patient identifiable information unless it is absolutely necessary**
Patient identifiable information items should not be used unless there is no alternative.
3. **Use the minimum necessary patient identifiable information**
Where use of patient identifiable information is considered to be essential, each individual item of information should be justified.
4. **Access to patient identifiable information should be on a strict need to know basis**
Only those individuals who need access to patient identifiable information should have access to it, and they should only have access to the information items that they need to see.
5. **Everyone should be aware of their responsibilities**
Action should be taken to ensure that those handling patient identifiable information - both clinical and non-clinical staff - are aware of their responsibilities and obligations to respect patient confidentiality.
6. **Understand and comply with the law**
Every use of patient identifiable information must be lawful. Someone in each organisation should be responsible for ensuring that the organisation complies with legal requirements.

Failure to maintain patient information in a confidential manner can result in disciplinary proceedings being taken against a member of staff.

12.5 WEEE Regulations

The Waste Electrical and Electronic Equipment Regulations 2006 (WEEE Regulations) came into force on 2nd January 2007. These regulations implement the European WEEE Directive in the United Kingdom.

In accordance with the WEEE regulations ASP will dispose of all ICT redundant equipment using a contracted company identified to do so.

When equipment is identified as no longer required, please contact the ASP ICT Service Desk to arrange collection.

The equipment will be removed to a designated secure location whilst waiting on-site wiping of data bearing components.

The process will include full tracking of equipment taken and confirmation of data cleansing. To facilitate this tracking, hard disk drives must NOT be removed from their host computer.

Unwanted items must be returned in as good a condition as is reasonably practical.