CHOOSE
YEOVIL HOSPITAL
HEALTH CARE

Information Security Policy

Version Number	3	Version Date	July 2013
Policy Owner	Chief Finance & Commercial Officer		
Author	Taunton & Somerset IT Services IT Manager		
First approval or date last reviewed	Jan 09		
Staff/Groups Consulted	Somerset Information Governance Group YDH Information Governance Steering Group		
Discussed by Policy Group	Jan 2009		
Approved by	Information Governance Steering Group		
Next Review Due	July 2016		
Policy Audited			
Equality Impact Assessment Completed	July 2013		

Table of Contents

Information Security Policy

1. RATIONALE

1.1. The Trust holds and manages a large amount of personal and confidential data relating to patients, the public and employees of the NHS. An ever increasing reliance is placed on computers to store and process this information. In addition, with the ever-easier ways by which information can be transferred via the trust and other connected networks, it is important that a consistent approach is adopted to safeguard the Trust's information. The approach needs to take into consideration the highly sensitive nature of some information held on both electronic and manual systems.

1.2. This document describes the trust's policy on information security and employees' responsibilities for security of information held on both electronic and manual systems.

The Information Security Policy addresses the following issues:

Confidentiality	Ensure that information is accessible only to those authorised to have access
Integrity	Safeguard the accuracy and completeness of information and processing to ensure confidence in the authenticity of the information
Availability	Ensure that authorised users have access to information and associated assets when required

1.3. The Trust is committed to maintaining and developing an information systems infrastructure, which has an appropriate level of security and data protection. All systems will have a minimum security framework.

1.4. Trust wide systems and their interfaces are managed by Taunton & Somerset IT Services on behalf of the Trust. In the case of departmental or stand alone systems it is the responsibility of the relevant Manager to ensure compliance with this policy.

2. SCOPE

This policy applies to:

- All Trust employees whilst engaged in work for the Trust at any location, on any manual system, computer system or Internet connection.

- Other persons working for the Trust, persons engaged on Trust business or persons using Trust equipment and networks.

- All usage by anyone granted access to the Trust network

3. DEFINITIONS

- **Data Controller** - The person or Trust that collects personal data and decides on how to use, store or distribute that data.

- **Data Processor** - Someone other than the Data Controller who processes personal data on their behalf.

- **Data Subject** - An individual who is the subject of the personal data.

- **Personal Data** - Data that relates to a living individual that can identify the individual from this data or other information in the possession of a data controller.

- **Relevant Filing System** - A structured set of information that can reference individuals either directly or indirectly.

4. ROLES AND RESPONSIBILITIES

Security is everybody's business and therefore it is everybody’s responsibility to ensure information is appropriate, confidential, accurate and available to authorised users. This section describes the different areas of responsibilities for ensuring that the Trusts data and IT assets remain secure.

4.1. Board of Directors

The Board of Directors has overall responsibility for all matters relating to security.

4.2. Directors and Business Managers

Directors and Business Managers should:

- Ensure that all current, new and temporary staff are educated in their security responsibilities and properly trained to use computer systems/media
- Determine which individuals are to be given authority to access specific information: levels of access to specific systems should be on a job function need, irrespective of job position
- Ensure that the IT Services Customer Service Desk is notified of new employees to allow access rights to be appropriately established from effective dates
- Authorise new manual information systems and regularly review, ensuring they provide an adequate level of security and do not compromise the existing infrastructure
- Implement procedures to minimise the Trust’s exposure to fraud, theft, or disruption of its systems; such as segregation of duties, dual control or staff rotation in critical susceptible areas
- Ensure that current documentation is always maintained for all critical job functions to ensure continuity in the event of individual unavailability

4.3. Information Governance Steering Group

The Information Governance Steering Group is responsible for the implementation and enforcement of the Information Security Policy and has total security management responsibility for:

- Monitoring and reporting on the state of Information Management & Technology (IM&T) security within the Trust
- Ensuring that the Information Security Policy is implemented throughout the Trust
- Developing and enforcing detailed procedures to maintain security
- Ensuring compliance with relevant legislation
- Ensuring that Trust personnel are aware of their responsibilities and accountability for information security
- Monitoring for actual or potential information security breaches
- Reporting security issues to the Trust Chief Executive through the Non Clinical risk Assurance Committee (NCRAC)
- Providing an advisory service on information security and information governance through the Information Governance Steering Group (i.e. Caldicott Guardian and Data Protection Officer)

4.4. Taunton & Somerset IT Services, IT Services Manager

The IT Services Manager should:

- Understand the risk to the computer assets and the information that is held on them.
- Deploy appropriate security measures to reduce the threat and to reduce the impact of a threat that materialises.
- Ensure periodic security reviews by systems managers at least once every year; the depth of a review will be determined by the importance, criticality and size of the particular system.
- Carry our annual risk assessments of all trust computer rooms and take any action necessary to prevent an incident of any kind. Risk Assessment should be made available to the IG Steering Group via the IT Services Manager
- Ensure that new information systems provide an adequate level of security and do not compromise the existing infrastructure
- Ensure that procedures are in place so that heads of departments advise Taunton & Somerset IT Services Customer Service Desk immediately of staff changes affecting computer access (for example job function changes / leaving department or Trust) so that passwords may be withdrawn / deleted
- Ensure that the Taunton & Somerset IT Services Customer Service Desk maintain security in line with the Information Security Policy.

4.5. Line Managers

Line Managers should:

- Ensure that staff are working in a manner consistent with the Information Security Policy.
- Investigate any security issue that members of staff raise in connection with their work.
- Address unresolved security issues with the Information Governance Lead.

4.6. Staff

Employees, including those under contract and agency staff should:

- Bring to their manager or Information Governance Lead's attention areas of concern regarding information security and breaches,
- Abide by the terms of the legislation detailed in the references
- Ensure they are familiar with anti-virus measures and that such software is being maintained with regular automated updates on their personal computer.

4.7. Security Incident Management

4.8. All staff are responsible for ensuring that no actual or potential security breaches occur as a result of their actions.

4.9. The Trust will investigate all suspected / actual security breaches and report them to the Information Governance Steering Group. The Taunton & Somerset IT Services Manager should be informed of all unresolved security issues in order to carry out the appropriate investigation.

5. RISK

5.1. Any security measures must be viewed as necessary as protection against a risk of an event occurring or to reduce the impact of such an event. Some of these events may be deliberate acts of damage and others may be accidental. Nevertheless, a range of security measures can be deployed to address:

- The threat of something affecting the confidentiality, integrity or availability of information held on systems or manual records.
- The impact that such a threat would have, if it occurred.
- The chance of such a threat occurring.

5.2. All staff should consider the risks associated with the computers and the information that is held on them, as well as information held in manual records

5.3. All staff are responsible for reporting any apparent shortcomings of security measures currently employed to address these risks to the Taunton & Somerset IT Services Manager.

6. ELECTRONIC AND MANUAL RECORDS

6.1. Physical Security

6.1.1. All access to computers located within Trust property must be restricted through the use of the same precautions that are taken for other valuable assets of the Trust. Such restrictions include layered security, making sure that security doors are closed properly, blinds drawn, and that any door entry codes are changed regularly. A safe haven should be made available if required.

6.1.2. Staff must wear identification badges and should challenge individuals not wearing identification anywhere in the trust grounds; visitors should be met at reception and accompanied at all times. Visitor books should be maintained at all times.

6.1.3. Only NHS owned and approved equipment is to be connected to the trust network. No personal or third party contractor equipment is to be connected to the trust network in any circumstances. Doing so will contravene the Trust Statement of Compliance which is the personal responsibility of the trust CEO.

6.1.4. Computers holding critical information should be located in rooms that have lockable doors. Staff on termination of employment or contract must surrender door keys, smart cards and ID badges and have their computer accounts suspended as soon as possible.

6.1.5. All computer assets including hardware and software must be recorded on an asset register that details the specification, user and location of the asset. See the Taunton & Somerset IT Services Inventory Policy. The IT Services Manager is responsible for ensuring that the trust inventory is properly maintained and regularly audited.

6.1.6. Computers must not be moved without notifying the Customer Service Desk in advance. Each machine will be security marked and its serial number recorded.

6.1.7. A computer must not connect, via cable or wireless to any network, including the Internet, without proper authorisation. Access to the local area network requires the form available on the Intranet to be completed and authorised and external access to trust systems should adhere to the Taunton & Somerset IT Services Remote Access Policy.

6.1.8. When IT equipment is removed from the Trusts premises, the user must take all reasonable care whilst it is in their possession. In particular, equipment must not be left visible in unattended cars in public places and consequently vulnerable to theft.

6.1.9. Any theft, or suspected theft, or any actual or suspected misuse must be reported to the Taunton & Somerset IT Services Customer Service Desk as soon as possible.

6.1.10. Employees should make every effort to ensure that fire, flood and accidents do not damage IT equipment.

6.1.11. Equipment must be sited to minimise the risk of accidental damage. Common hazards include drinks, food and the straining of leads when a machine is moved.

6.1.12. No paper should be stored on or near computer equipment due to the risk of fire; computers generate a lot of heat in use and need adequate ventilation.

6.1.13. Any suspected damage, which may not be visible externally (for example after dropping a computer), must be reported to the Taunton & Somerset IT Services Customer Service Desk for checking before continued use.

6.2. Disposal of Equipment and Media

6.2.1. Computer assets must be disposed of in accordance with the IT Services disposal policy. This includes removable computer media, such as tapes, disks and printed reports.

6.2.2. All data storage devices will be purged of sensitive data before disposal. Where this is not possible, due to quantities involved the equipment or media will be destroyed by a technical waste service provider. The Taunton & Somerset IT Services Customer Service Desk should be contacted for further details.

6.3. Computer Equipment Security

6.3.1. To avoid interruption to business activity, IM&T equipment will be protected against loss or damage through the use of environmental controls which will be installed to protect critical equipment.

6.3.2. All critical processing equipment, including file servers, are housed in a secure computer room at all times and will be covered by third party support and maintenance agreements.

6.4. Information Storage and Back up

6.4.1. No information must be held that breaches the Data Protection Act 1998 or formal notification and guidance issued by the Department of Health.

6.4.2. All staff must comply with data protection legislation and must not be allowed to access information until line managers are satisfied that they understand and agree these responsibilities.

6.4.3. Information that is no longer required should be disposed or archived securely and in line with the Records Management Strategy. Paper records containing personal information must be disposed of securely. Anything containing personal and/or confidential information that does not require archiving must be shredded after use. Any confidential information must be placed out of sight, preferably in locked cabinets when not in use.

6.4.4. Sensitive information must not be stored on individual drives on PCs or Laptops. This information is to be stored on the network servers where available, with restricted access. This will maintain confidentiality, availability and integrity of that information and reduce impact of breaches in physical security. Should a need arise for local storage the Taunton & Somerset IT Services Customer Service Desk must be contacted to advise on adequate physical security and backup arrangements.

6.4.5. Data located upon critical network servers will be backed up in accordance with the written back-up procedures to provide at least one month information retention. Such information will be stored off-site, as required, to facilitate a maximum loss of one calendar week of information destroyed as a result of system damage

6.4.6. All back-ups will be maintained securely and will be erased when no longer required

6.4.7. If information is copied between systems within the network, employees should ensure that any confidential information remains secure and that the recipient system has the same or greater standard of security protection as the first.

6.5. Data Encryption

6.5.1. The Cabinet Secretary has directed that there should be no transfers of unencrypted person identifiable data held in electronic format across the NHS. Any such data stored on a PC or other removable device in a non-secure area or on a portable device such as a laptop, PDA or mobile phone should also be encrypted. This is now a requirement across all public sector organisations.

6.5.2. The first rule to obey is that person identifiable data should never be downloaded from a networked computer system and stored on a Trust personal desktop computer, a laptop computer or any removable storage device, such as USB memory sticks, unless the person doing so is a Trust Registered Data Mover. A register of Trust Registered Data Movers is kept and maintained by the Trust Information Governance Lead.

6.5.3. All high risk PCs and Laptops should be protected by the Safeboot encryption tool, sourced by the DoH.

6.6. Encrypting Email

6.6.1. Messages sent from Outlook Mail service to any County wide NHS organisation will be automatically encrypted. Messgaes sent outside of this area should have the word “ENCRYPT” in the subject line.

6.6.2. NHSmail is encrypted from end to end only if sent to another NHSmail user, if a user of NHSmail sends an email to a non-NHSmail user, the encryption will be disabled.

6.7. Business Continuity Planning

6.7.1. All systems will have threats and vulnerabilities assessed to determine how critical they are to the trust. All critical systems will have a written back-up procedure and a disaster recovery plan. This is required to counteract interruptions to business activities and to protect critical business processes from the effects of major failures or disasters.

6.7.2. Individual departments should have procedures in place to maintain essential services in the event of IT system failure. Details of these arrangements can be found in the Business Continuity Plan.

6.8. System Ownership

6.8.1. Each designated critical and sensitive system will have a trust nominated “system owner” and a nominated Taunton & Somerset IT Services systems manager, and both must ensure compliance with the Information Security Policy, ensuring the appropriate use of equipment, support and maintenance.

6.9. Networks Management

6.9.1. Through connection to the Trust's network it is possible to receive and forward information to other users on the network and to other Trust networks using, for example, electronic mail. Should employees receive, or gain access to unauthorised information on any networks then this event must be reported to the Taunton & Somerset IT Services Information Services Manager.

6.9.2. A security log must be maintained for any access to the Trust's network by external organisations. The Taunton & Somerset IT Services Customer Service Desk will hold this log.

6.9.3. All computer files, transferred from other networks (including public access networks such as the Internet) and removable media must be checked for viruses before use within the Trust. Files stored on the network will be checked daily.

6.9.4. Equipment should not be used until advised by the installation technician that the system is ready for use.

6.9.5. Staff must inform the Taunton & Somerset IT Services Customer Service Desk if a virus attack is detected or suspected.

6.10. User Access to Network, Computers and Applications

6.10.1. Only Trust staff and authorised third parties are authorised to access Trust computers and the information held on them. Unauthorised access may contravene the Computer Misuse Act 1990 and Data Protection Act 1998 leaving the user open to prosecution.

6.10.2. The access control policy will take account of security requirements of the business application and will be granted only on approval of an application by the relevant systems manager.

6.10.3. No individual will be given access to a live system unless properly authorised, trained and made aware of his or her security responsibilities.

6.10.4. Remote access to the network will be protected by passwords and strong authentication. Employees must only be granted access to those areas that they require to perform their duties and this access should be reviewed by Heads of Department on a regular basis, but at least annually.

6.11. Notification of Staff Changes

6.11.1. Managers will be responsible for notification of new employees to the Taunton & Somerset IT Services Customer Service Desk to allow access rights to be appropriately established from effective dates.

6.11.2. The Payroll department will provide a leavers list each month to advise the Customer Service Desk about staff changes affecting computer access (for example job function changes / leaving department or Trust) so that access rights may be amended, suspended or deleted, from the effective dates.

6.12. Security of third party access to NHS Networks

6.12.1. Written agreement must be received from all external contractors and non-NHS parties that they agree to treat all information confidentially and that information will not be disclosed to unauthorised individuals. Such contractors should also sign a declaration that they understand the relevant legislation should they need to access sensitive information stored on a computer system.

7. USER RESPONSIBILITIES

7.1. Use and Installation of Software

7.1.1. Under no circumstances should software, other than that approved and authorised, be loaded onto Trust's computers. Staff must not bring or download software onto Trusts premises without first seeking permission from their head of department and informing the Customer Service Desk.

7.1.2. It is a criminal offence to make/use unauthorised copies of commercial software and offenders are liable to prosecution

7.1.3. All changes to and the installation of software programs may only be undertaken under the direction of the IT Services Manager.

7.1.4. Games Software, except for the purpose of authorised training is not permitted for use on Trust's equipment and must not be installed or used on the premises.

7.2. Computer viruses

7.2.1. Software and information processing facilities are vulnerable to the introduction of malicious software, such as computer viruses.

7.2.2. Virus threats are a day-to-day threat however the type, strain, and number of incidents may well increase due to increased Internet activity. This can cause serious disruption to both the user other trust employees, patients and the IT Support Teams.

7.2.3. All the Trust's personal computers must run anti-virus software

7.2.4. Staff should not use computer media that has not been checked for viruses. Staff should not send computer media to external addresses without checking them for viruses. Staff must contact the Customer Service Desk if a virus incident is suspected.

7.3. Password Guidance

7.3.1. Passwords have a valuable role in protecting systems from unauthorised access and are most effective when they:

- carry no meaning
- are not names or have other connections to the user
- are changed regularly and are not related to previous passwords
- are a minimum of 8 characters
- are a mixture of letters, numbers and symbols
- are kept secret
- are not 'VISITOR', 'GUEST' Birthday, or similar
- are not shared

7.3.2. Passwords used within the Trust's systems must be a minimum of 8 characters; they must be changed at least every 90 days and deleted when a user no longer requires access to the system. A default password is used for new accounts set-up. The user will then be prompted to change the password.

7.3.3. Only the person to whom it is issued should use that password. Employees must never divulge a password.

7.3.4. Only in exceptional circumstances and not without agreement of senior management will IT Services change a password to grant temporary access, after-which, a new password will be generated before further access to system.

7.3.5. IT Services are not permitted to change email system passwords of staff who have left the organisation, so that management can gain access to the email account, unless written authority of the user who has left is provided. Data Protection Act 1998 refers.

7.4. Clear Screen Policy

Workstations will require a username and password to be entered before accessing any software on that machine, where the operating system permits. Windows screen saver with password protection enabled will be used on all PCs with time out set to twenty minutes within sensitive locations and a maximum of thirty minutes at other locations.

7.5. Clear Desk Policy

Any confidential information must be placed out of sight, in locked cabinets when not in use.

7.6. Personal Use of Trust Systems

Trust systems are not to be used for personal use. All computer equipment leaving the Trust's premises should be authorised by the line manager and a log kept of the disposal.

7.7. Management of Manual Records

Storing, archiving and disposing of manual records will be dealt with in accordance with the Records Management Strategy Policy.

7.8. Relevant Filing System

The Data Protection Act 1998 covers not only personal data attributable to a living person held in an automatically processed form but also personal information which is recorded as part of a 'relevant filing system'. Information recorded as part of a 'relevant filing system' is a structured set of information that can reference individuals either directly or indirectly so that 'specific information relating to a particular individual is readily accessible'. This definition covers some types of paper-held data.

7.9. Sharing of Personal Information

Information relating to individuals should not be shared without following the Guidance for Sharing Information by Fax, Phone or Post.

8. INTERNET & EMAIL

8.1. Internet Access

8.1.1. The trust regards the Internet as a tool for managing and delivering services and as a useful mechanism for the open exchange of ideas and non-confidential sources of information between its employees, other members of the NHS and the public.

8.1.2. However, the Internet is a hostile network and if not used sensibly and appropriately could be very damaging for the trust. Inappropriate use can introduce viruses and other damaging software to the trust networks and networked devices causing system downtime and a waste of trust resources.

8.1.3. The Internet can also be a wasteful resource in terms of the amount of time that it could consume if not used wisely or appropriately. Staff using the Internet must ensure they comply with the Trust's Internet Access Policy.

8.2. Use of Email

8.2.1. All staff should be aware that misuse of the trust email system is a disciplinary offence.

8.3. All users should protect their email account with a password. Only IT Services, with instructions from a trust director are permitted to change an email password to allow access by another person or persons.

8.4. Staff using the email system must comply with the trust Email Policy

8.5. Information Security - Contact Information

The IT Services Manager provides support and guidance to the Trust on all issues concerning information security and information governance matters, such as Data Protection and Caldicott Guidance. The IT Services Manager can be contacted via the Customer Service Desk:

Customer Service Desk	Telephone: 01823 28 77 28

9. LIMITATIONS

9.1. This policy and procedure will apply to all staff employed, voluntary or undergoing training at Yeovil District Hospital NHS Foundation Trust.

9.2. This policy will form part of the Standing Orders of the Trust and will be included in the Schedule to the written particulars of employment of all staff employed by the Trust.

10. IMPLEMENTATION, MONITORING AND EVALUATION

Implementation, monitoring and evaluation will be in accordance with the Trust Policy on Policies.

ANNEX A – GUIDANCE FOR SHARING PERSONAL INFORMATION

Introduction

There are a number of different methods used for sharing personal information (about staff and patients) within the NHS (and in relation to patient care it maybe necessary to share information with other NHS and non-NHS bodies e.g. social services, police authorities, education authorities). It is essential that this confidential information is kept secure and adheres to the Data Protection Principles and the Caldicott Principles.

This practical guidance provides all staff with firm direction in the methods of sharing information related to postal, telephone or fax of personal information. In addition guidance is provided on how information should be transported. It also highlights which principles are being adhered to when this guidance is put into practice.
Guidance for Sharing Information by Post or other Delivery Service

- Confirm the name, department and address of the recipient.
- Seal the information in a robust envelope.
- Mark the envelope “Private and Confidential-To be opened by addressee only.”
- When appropriate send the information by recorded delivery.
- When necessary ask the recipient to confirm receipt.

Data Protection Principles 6 and 7. Caldicott Principle 4.

Guidance for Sharing Information by Transportation (Manual Records)

- Personal identifiable information should only be taken off site when absolutely necessary, or in accordance with local policy.
- Record what information you taking off site and why, and if applicable, where and to whom you are taking it.
- Information must be transported in a sealed container.
- Never leave personal identifiable information unattended or on view in vehicles.
- Ensure the information is returned back on site as soon as possible.
- Record that the information has been returned.

Data Protection Principle 7.Caldicott Principles 4 and 6.

Fax Machines

- Fax machines must only be used to transfer personal information where it is absolutely necessary to do so. The following must apply:
- Ensure it is sited in an area that is restricted to those who need to access the information
- The fax is sent to a safe location where only staff that has a legitimate right to view the information can access it
- The sender is certain that the correct person will receive it and that the fax number is correct
- Notify the recipient when the fax is sent and ask them to acknowledge receipt
- The confirmation of receipt should be checked to ensure the fax has been transmitted to the intended recipient. Where possible this should be attached to the original document

- Where possible the NHS number should be used for identification in preference to the patients name and address
- Only the minimum amount of personal information should be sent
- Care is taken in dialling the correct number
- All confidential faxes sent should be clearly marked ‘Private and Confidential’ on the front sheet
- Frequently used numbers should be programmed into the fax machine ‘memory dial’ facility. This will minimise the risk of dialling incorrect numbers
- In clinical areas the Safe haven should be in a room/area where any incoming fax letters or emails can be received in privacy and retrieved only by authorised personnel
- If you receive a call requesting that confidential information be sent via fax always call the requestor back to confirm the caller’s identity using an independent number source
- Always seek advice from your line manager or the Information Governance team if you are unsure whether or not to send any information via fax
- If it is highly sensitive ensure someone is a the receiving end waiting for it
- Ensure only authorised staff handle confidential information
- If you receive faxes that contain personal information store them in a secure environment
- Fax machines should be turned off out of hours.

Post

- Incoming mail should be opened away from public areas
- Outgoing mail (both internal and external) should be sealed securely and marked private and confidential if it contains person-identifiable information
- Where possible send post to a named person
- When sending documents by external post or courier, use a ‘signed for’ delivery service. Use appropriate stationery, such as reinforced envelopes or document wallets when necessary. Check that the address is typed or written clearly in indelible ink
- When sending outside the NHS send documents only to know, named, authorised personnel marked ‘Confidential’
- Use as risk assessment and register if appropriate

Paper Documents

- All sensitive records must be stored face down in public areas and not left unsupervised at any time
- Information that is no longer required ie: post it notes, messages, should be shredded or disposed of under confidential conditions
- Make a log of what notes have left the department ie: home visits etc
- Ensure that documents are properly ‘booked out’ of any relevant filing system if necessary, and records kept of what is sent and where. Copies should be sent or retained as appropriate

Computers

- Do not share log-ons and passwords with anyone
- Computer screens must not be left on view so members of the general public or staff who do not have a justified need to view the information can see personal data
- PC’s or laptops should be locked or switched off when you are away from your desk for any length of time
- Information should be held on the organisation’s network servers not stored on local hard drive or removable media
- Information must **not** be copied into any PC or media that is ‘outside the NHS’

- All person-identifiable information sent by email **must** be sent from one NHS mail address to another secure email domain such as NHS.net to NHS.net or via an encryption attachment

Telephone Calls

- Do not make telephone calls where you can be overheard ie in a reception area
- When you receive a call check to ensure you are speaking to the correct person, ring back where possible to confirm someone's identity

APPENDIX 1 – EQUALITY IMPACT ASSESSMENT TOOL

To be completed and attached to any procedural document when submitted to the appropriate committee for consideration and approval.

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

If you have identified a potential discriminatory impact of this procedural document, please refer it to Yeovil Academy, together with any suggestions as to the action required to avoid/reduce this impact.

Name: Karen Carter Date: 16 July 2013