The

MAST

Academy Trust

Policy	Information Security Policy
Owner	Melanie Humphreys – The Mast Executive Administrator
Date approved	1st March 2021
Approver	Trust Board Audit Committee

Current version	V2.0
Next review due	Spring term 2024

Objective of Policy

This Security Policy document summarises what is expected of all Mast Academy Trust employees in the course of their duties and while on school premises and/or working from home.

Its aim is to protect the Trust's pupils, parents, employees, assets (including information assets), finances and reputation by reducing the risk of:

- Harm to individuals
- Accidental loss or damage to assets
- Unintended change to, or disclosure of, personal and confidential information
- Deliberate and harmful acts carried out through lack of awareness of their consequences

It applies to:

- All services of the Trust
- All employees of the Trust, both permanent and temporary
- All volunteers for the Trust, including Members, Trustees and Governors
- Any other person, or organisation, working for the Trust or on Trust premises

This policy document provides the information necessary to enable staff and others to meet their general responsibility to safeguard the Trust's information and other assets

Version Control	
Version Number	Summary of amends from previous version
2.0	Development of the policy to Trust version

Sign off requirements	
Approvers	Position
Audit Committee	Trust Board
Reviewers	Position
Jason Field	CFO The MAST
Philip Oldfield	Trustee

1.0 Introduction

1.1. This policy applies to all staff (which includes Governors, agency staff, contractors, work experience students and volunteers) when handling Personal Data. For more information on what Personal Data is, please see Mast Academy Trust's data protection policy.

1.2. Any questions or concerns about your obligations under this policy should be referred to the Trust Operations Officer. swalters@themast.co.uk

1.3. Any reference to personal data in this document means private information, whether in electronic or written form, about identifiable pupils, parents, employees, members of the public or any other persons. Sensitive personal data includes sensitive information about a living, identifiable individual for example, information which relates to their racial or ethnic origin, political beliefs or to their physical or mental health.

2.0 Be aware

2.1. Information security breaches can happen in a number of different ways. Examples of breaches include:

2.1.1.1. an unencrypted laptop stolen after being left on a train;

2.1.1.2. Personal Data taken after website was hacked

2.1.1.3. sending a confidential email to the wrong recipient; and

2.1.1.4. leaving confidential documents containing Personal Data on a doorstep.

2.2. You should immediately report all security incidents, breaches and weaknesses to the Headteacher or Trust Operations Officer. This includes anything which you become aware of even if you are not directly involved (for example, if you know that document storage rooms are sometimes left unlocked at weekends).

2.3. You must immediately tell the Headteacher or Trust Operations Officer and the IT Department if you become aware of anything which might mean that there has been a data protection or security breach.

This could be anything which puts Personal Data at risk, for example, if Personal Data has been or is at risk of being destroyed, altered, disclosed or accessed without authorisation, lost or stolen. You must provide your Headteacher or the Trust Operations Officer with all of the information you have.

All of the following are examples of a security breach:

2.3.1.1. you accidently send an email to the wrong recipient;

2.3.1.2. you cannot find some papers which contain Personal Data; or

2.3.1.3. any device (such as a laptop or a smartphone) used to access or store Personal Data has been lost or stolen or you suspect that the security of a device has been compromised.

2.4. In certain situations The Mast Academy Trust must report an information security

breach to the Information Commissioner's Office (the data protection regulator) and let those whose information has been compromised know within strict timescales. This is another reason why it is vital that you report breaches immediately.

3.0 Thinking about privacy on a day to day basis

3.1. You must consider data protection and privacy whenever handling Personal Data.

3.2. In some situations, the Mast Academy Trust is required to carry out an assessment of the privacy implications of using Personal Data in certain ways. For example, when new technology is introduced, where the processing results in a particular risk to an individual's privacy.

3.3. These assessments should help the Mast Academy Trust to identify the measures needed to prevent information security breaches from taking place.

4.0 Critical Personal Data

4.1. Critical Personal Data is:

- information concerning child protection matters;
- information about serious or confidential medical conditions and information about special educational needs;
- information concerning serious allegations made against an individual (whether or not the allegation amounts to a criminal offence and whether or not the allegation has been proved)
- financial information (for example about parents and staff)
- information about an individual's racial or ethnic origin; and
- political opinions;
- religious beliefs or other beliefs of a similar nature;
- trade union membership;
- physical or mental health or condition;
- genetic information;
- sexual life or sexual orientation;
- information relating to actual or alleged criminal activity; and
- biometric information (e.g. fingerprints used for controlling access to a building).

Staff need to be extra careful when handling Critical Personal Data.

5.0 Minimising the amount of Personal Data that we hold

5.1. Restricting the amount of Personal Data we hold to that which is needed helps keep personal data safe. Never delete personal data unless you are sure you are allowed to do so.

6.0 Using computers and IT

6.1. Lock computer screens: Your computer screen should be locked when it is not in use, even if you are only away from the computer for a short period of time.

6.2. Be familiar with the Mast Academy Trust IT: Familiarise yourself with any software or hardware that you use. In particular, make sure that you understand what the software is supposed to be used for and any risks. For example:

6.2.1. if you use a "virtual classroom" which allows you to upload lesson plans and mock exam papers for pupils then you need to be careful that you do not accidently upload anything more confidential;

6.2.2. make sure that you know how to properly use any security features contained in software. For example, some software will allow you to redact documents (i.e. "black out" text so that it cannot be read by the recipient). Make sure that you can use this software correctly so that the recipient of the document cannot "undo" the redactions; and

6.2.3. be careful where you store information containing Critical Personal Data. For example, safeguarding information should not be saved on a shared computer drive accessible to all staff.

6.3. Hardware and software not provided by The Mast Academy Trust: Staff must not use, download or install any software, app, programme, or service without permission from the IT team. Staff must not connect (whether physically or by using another method such as Wi-Fi or Bluetooth) any device or hardware to schools IT systems without permission.

6.4. Private cloud storage: You must not use private cloud storage or file sharing accounts to store or share Trust or school documents.

6.5. Portable media devices: The use of portable media devices (such as USB drives, portable hard drives, DVDs) is not allowed unless those devices have been given to you by the Trust/school and you have received training on how to use those devices securely. The IT team will protect any portable media device given to you with encryption.

6.6. The Mast Academy Trust IT equipment: If you are given Mast Academy Trust IT equipment to use (this includes laptops, printers, phones, and DVDs) you must make sure that this is recorded on Mast Academy Trust's IT equipment asset register. Mast Academy Trust IT equipment must always be returned to the IT team even if you think that it is broken and will no longer work and the asset register updated accordingly.

6.7. Where to store electronic documents and information: You must ensure that you only save or store electronic information and documents on secure drives.

7.0 Passwords

7.1. Passwords should be long and difficult to guess. Do not choose a password which is so complex that it's difficult to remember without writing it down. Your password should not be disclosed to anyone else.

7.2. You should not use a password which other people might guess or know, or be able to find out, such as your address or your birthday.

7.3. You must not use a password which is used for another account. For example, you must not use your password for your private email address or online services for any school account.

7.4. Passwords (and any other security credential you are issued with such as a key fob or USB drive) must be kept secure and confidential and must not be shared with, or given to, anyone else. Passwords should not be written down.

8.0 Emails (and faxes)

8.1. When sending emails or faxes you must take care to make sure that the recipients are correct.

8.2. If the email (or fax) contains Critical Personal Data then you should ask another member of staff to double check that you have entered the email address / fax number correctly before pressing send. If a fax contains Critical Personal Data then you must make sure that the intended recipient is standing by the fax machine to receive the fax.

8.3. Encryption: Remember to encrypt internal and external emails which contain Critical Personal Data. For example, WORD documents can be attached to email and encrypted with a password which can then be forwarded separately to the recipient.

8.4. Private email addresses: You must not use a private email address for Mast Academy Trust related work. You must only use your school address. Please note that this rule also applies to Trustees and Governors.

9.0 Paper files

9.1. Keep under lock and key: Staff must ensure that papers which contain Personal Data are kept under lock and key in a secure location and that they are never left unattended on desks (unless the room is secure). Any keys must be kept safe.

9.2. If the papers contain Critical Personal Data then they must be kept in secure cabinets identified for the specified purpose as set out in the table below. Information held in paper form must not be stored in any other location, for example, child protection information should only be stored in the cabinet in the Designated Safeguarding Lead's (DSL) room.

Cabinet	**Access**

Child protection - located in the DSL's office	CEO, Headteacher and DSL
Financial information	School – Headteacher and School Business Manager Trust - CEO, CFO and Finance Officer
Health information and Single Central Register Information etc	School – Headteacher, Headteacher's PA and School Business Manager Trust - CEO, CFO and Executive Administrator

9.3. Disposal: Paper records containing Personal Data should be disposed of securely shredding the material. Personal Data should never be placed in the general waste.

9.4. Printing: When printing documents, make sure that you collect everything from the printer straight away, otherwise there is a risk that confidential information might be read or picked up by someone else. If you see anything left by the printer which contains Personal Data then you must hand it in to the school office.

9.5. Put papers away: You should always keep a tidy desk and put papers away when they are no longer needed. Staff are provided with their own personal secure cabinet(s) in which to store papers. However, these personal cabinets should not be used to store documents containing Critical Personal Data. Please see paragraph 9.2 above for details of where Critical Personal Data should be kept.

9.6. Post: You also need to be extra careful when sending items in the post. Confidential materials should not be sent using standard post. If you need to send something in the post that is confidential, consider asking your IT team to put in on an encrypted memory stick or arrange for it to be sent by courier.

10.0 Working off site (e.g. school trips and homeworking)

10.1. Staff might need to take Personal Data off the site for various reasons, (for example because they are working from home or supervising a school trip]. This does not breach data protection law if the appropriate safeguards are in place to protect Personal Data.

10.2. For school trips, the trip organiser should decide what information needs to be taken and who will be responsible for looking after it. You must make sure that Personal Data taken off site is returned to Mast Academy Trust or the school.

10.3. If you are allowed to work from home then check with the Trust Operations Officer what additional arrangements are in place. This might involve working with a specially encrypted memory stick or installing software on your home computer or smartphone: see section 11 below. (Not all staff are allowed to work from home)

10.4. Take the minimum with you: When working away from your school you must only take the minimum amount of information with you.

10.5. Working on the move: You must not work on documents containing Personal Data whilst travelling if there is a risk of unauthorised disclosure (for example, if there is a

risk that someone else will be able to see what you are doing). For example, if working in a public place, you should ensure that no one else can see the laptop screen and you should not leave any device unattended where there is a risk that it might be taken.

10.6. Paper records: If you need to take hard copy (i.e. paper) records with you then you should make sure that they are kept secure. For example:

10.6.1. documents should be kept in a locked case. They should also be kept somewhere secure in addition to being kept in a locked case if left unattended (e.g. overnight);

10.6.2. if travelling by public transport you must keep the documents with you at all times and they should not be stored in luggage racks;

10.6.3. if travelling by car, you must keep the documents out of plain sight.

10.6.4. if you have a choice between leaving documents in a vehicle and taking them with you (e.g. to a meeting) then you should usually take them with you and keep them on your person in a locked case. However, there may be specific circumstances when you consider that it would be safer to leave them in a locked case in the vehicle out of plain sight. The risks of this situation should be reduced by only having the minimum amount of Personal Data with you (please see 10.4 above).

10.7. Public Wi-Fi: You must not use public Wi-Fi to connect to the internet. For example, if you are working in a cafe then you will either need to work offline or use 3G / 4G.]

10.8. Using Mast Academy Trust laptops, phones, cameras and other devices: If you need to book out an Mast Academy Trust device then save all data on a specially encrypted memory stick which remains the property of Mast Academy Trust.

10.9. Critical Personal Data should not be taken off the site in paper format save for specified situations where this is absolutely necessary (see 10.4 above).

11.0 Using personal devices for school/Trust work

11.1. You must only use a Trust or School issued laptop or tablet for your school work. Personal devices of this nature should not be used for school related business unless express permission of the Headteacher or Trust Operations Officer has been sought.

11.2. You may only use your personal smartphone for school work if you have been given permission by the Headteacher or Trust Operations Officer

11.3. If you have been given permission then before using your own device for school work you must speak to your IT team so that they can ensure your device has the appropriate security measures such as biometric identity or passcodes.

11.4. When using your personal smartphone for work you must do so in conjunction with the Trust's best practice guidance for use of mobile phones for work purposes.

11.5. If using your smartphone for work emails you must do this using a specific app for the email platform you are accessing eg Office 365. Emails must not be accessed via

your phone's generic email system.

11.6. Appropriate security measures should always be taken. This includes the use of firewalls and anti-virus software. Any software or operating system on the device should be kept up to date.

11.7. Default passwords: If you use a personal device for school work which came with a default password then this password should be changed immediately. Please see section 7 above for guidance on choosing a strong password.

11.8. Sending or saving documents to your personal devices: Documents containing Personal Data (including photographs and videos) should not be sent to or saved to personal devices, unless you have been given permission by the Headteacher or Trust Operations. This is because anything you save to your computer, tablet or mobile phone will not be protected by Mast Academy Trust's security systems.

11.9. Friends and family: You must take steps to ensure that others who use your device (for example, friends and family) cannot access anything school related on your device. For example, you should not share the login details with others and you should log out of your account once you have finished working by restarting your device. You must also make sure that your devices are not configured in a way that would allow someone else access to school related documents and information.

11.10. When you stop using your device for school work: If you stop using your device for school work, for example:

11.10.1. if you decide that you do not wish to use your device for school work; or

11.10.2. if the school withdraws permission for you to use your device; or

11.10.3. if you are about to leave Mast Academy Trust

then, all school documents (including school emails), and any software applications provided by us for school purposes, will be removed from the device.

If this cannot be achieved remotely, you must submit the device to the IT team for wiping and software removal. You must provide all necessary co-operation and assistance to the IT team in relation to this process.

12.0 Breach of this policy

12.1. Any breach of this policy will be taken seriously and may result in disciplinary action.

12.2. A member of staff who deliberately or recklessly obtains or discloses Personal Data held by Mast Academy Trust or their schools without proper authority is also guilty of a criminal offence and gross misconduct. This could result in summary dismissal. Further information on this and on other offences can be found in Mast Academy Trust's data protection policy found on the Trust website.

12.3. This policy does not form part of any employee's contract of employment.

12.4. We reserve the right to change this policy at any time. Where appropriate, we will notify staff of those changes by mail or email.

13.0 More Information

13.1. The following policies that relate to this policy can be found on the Trust website:

- Data protection policy
- ICT and acceptable usage policy
- Whistleblowing policy
- Best practice guidance

14.0 Legal Context

Data Protection Act 2018
Defines personal data and regulates all aspects of its use and processing.

General Data Protection Regulation 2018
The General Data Protection Regulation 2016/679 is a regulation in EU law on data protection and privacy in the European Union and the European Economic Area.

Computer Misuse Act 1990
Prohibits unauthorised access to computer material, unauthorised access with intent commit or facilitate commission of further offences, and unauthorised modification of computer material.

Copyright, Designs and Patents Act 1988
Covers the copying of proprietary software.

Regulation of Investigatory Powers Act 2000
Part III: Investigation of electronic data.

APPEDNIX A: Protocols and Guidance for the use of Mobile Phones in School

Personal mobile phones and mobile devices

Responsibility

- Mobile phones and personally-owned mobile devices brought into school are entirely at the staff member, pupil's & parents' or visitors own risk. The Trust/school accepts no responsibility for the loss, theft or damage of any phone or hand held device brought into school
- The recording, taking and sharing of images, video and audio on any mobile phone is prohibited; except where it has been explicitly agreed otherwise by the Headteacher. Such authorised use is to be monitored and recorded. All mobile phone use is to be open to scrutiny and the CEO/ Headteacher is to be able to withdraw or restrict authorisation for use at any time if it is to be deemed necessary.
- Mobile phones and personally-owned devices approved for use by the CEO/Headteacher in exceptional circumstances are not permitted to be used in certain areas within the school site, e.g. changing rooms and toilets.

Staff

- Staff members may use their phones during school break times in certain areas. If a staff member is expecting a personal call they may leave their phone with the school office to answer on their behalf, or seek specific permissions to use their phone at other than their break times.
- Mobile phones and personally-owned devices will not be used in any way during lessons or formal school time. They should be switched off or silent at all times.

Staff use of personal devices

- Staff are not permitted to use their own mobile phones or devices for contacting children, young people or their families within or outside of the setting in a professional capacity.
- Staff will be issued with a school phone where contact with pupils, parents or carers is required. Staff will also be issued with a school phone whilst on educational off-site visits. Alternatively, staff may have permission from the Headteacher or the Educational Visits Co- ordinator to bring their own mobile phones on trips – to be used strictly for communication with the school or for emergency situations.
- Approved by CEO/Headteacher mobile phones and personally-owned devices will be switched off or switched to 'silent' mode. Bluetooth communication should be 'hidden' or switched off and mobile phones or personally-owned devices will not be used during teaching periods unless permission has been granted by a member of the senior leadership team in emergency circumstances.

- If members of staff have an educational reason to allow children to use mobile phones or a personally-owned device as part of an educational activity then it will only take place when approved by the senior leadership team.
- Staff should not use personally-owned devices, such as mobile phones or cameras, to take photos or videos of pupils and will only use work-provided equipment for this purpose.
- If a member of staff breaches the school policy then disciplinary action may be taken.
- Where staff members are required to use a mobile phone for school duties, for instance in case of emergency during off-site activities, or for contacting pupils or parents, then a school mobile phone will be provided and used. In an emergency where a staff member doesn't have access to a school-owned device, they should use their own device and hide (by inputting 141) their own mobile number for confidentiality purposes.

Visitors

- All visitors are requested to keep their phones on silent.

Parents and Pupils

- Where parents or pupils need to contact each other during the school day, they should do so only through the School's telephone.
- Mobile phones will not be used during lessons or formal school time unless as part of an approved and directed curriculum-based activity with consent from a member of staff.
- The Bluetooth or similar function of a mobile phone should be switched off at all times and not be used to send images or files to other mobile phones.
- No images or videos should be taken on mobile phones or personally-owned mobile devices without the prior consent of the person or people concerned.

Pupils' use of personal devices

- Refer to school mobile phone policy

Digital images and video in school:

- We gain parental / carer permission for use of digital photographs or video involving their child as part of the school agreement form when their daughter / son joins the school;
- We do not identify pupils in online photographic materials or include the full names

of pupils in the credits of any published school produced video materials / DVDs;

- Staff sign that they have read the school's full Information Security Policy and this includes a clause on the use of mobile phones / personal equipment for taking pictures of pupils;
- If specific pupil photos (not group photos) are used on the school web site, in the prospectus or in other high profile publications the school will obtain individual parental or pupil permission for its long term use
- The school blocks/filter access to social networking sites or newsgroups unless there is a specific approved educational purpose:

    - Pupils are taught about how images can be manipulated in their e-safety education programme and also taught to consider how to publish for a wide range of audiences which might include Directors, parents or younger children as part of their ICT scheme of work;
    - Pupils are advised to be very careful about placing any personal photos on any 'social' online network space. They are taught to understand the need to maintain privacy settings so as not to make public, personal information.
    - Pupils are taught that they should not post images or videos of others without their permission. We teach them about the risks associated with providing information with images (including the name of the file), that reveals the identify of others and their location, such as house number, street name or school. We teach them about the need to keep their data secure and what to do if they are subject to bullying or abuse.

APPENDIX B Information security responsibilities

Organisational Security	Responsibility
The Trust Board has a central custodian role on information security matters.	Trustees
Executive teams are responsible for implementing policy and advice.	CEO CFO
The Audit Committee will direct, review, support and approve Information Security campaigns, advice and overall responsibilities. Its responsibilities are: • to recognise opportunities and risks • to flag up issues of concern • to coordinate effort • to review advice	CEO CFO
All leaders must ensure that those who report to them are aware of their general responsibilities in respect of security and the value of information, and of any issues or risks specific to their areas of responsibility.	All leaders
Information security should be a regular item on team meeting agendas to ensure that issues of concern are highlighted and addressed.	All leaders

Personal Security	Responsibility
General responsibility for information security will be included in contracts of employment.	School/Collaborative team
Checks on the career history (including criminal records) of job applicants will be made, appropriate to the responsibilities of the job.	School/Collaborative team
Contractual arrangements with staff agencies will require similar, appropriate checks on agency staff.	School/Collaborative team
External contractors, consultants, trainers and others employed on Trust premises or given access to Trust systems must be subjected to checks and agreements appropriate to the services to be provided.	School/Collaborative team
Work placements, students, volunteers, partners and any other persons not subject to the contract of employment, and having access to Trust premises and/or systems, will be required to sign	School/Collaborative team

confidentiality and security agreements.	
A record will be made of equipment, fobs, etc, issued to new employees and any of the above.	ICT
Induction training will include security and data protection.	Line Managers
Staff will wear ID badges at all times (unless otherwise agreed in certain circumstances).	All staff
On change of employment, access to computer systems and Trust property issued should be reviewed and returned or cancelled where appropriate. On termination of employment, all Trust property must be returned or accounted for, and computer system access cancelled.	Line managers

Security of Information	**Responsibility**
It must not be assumed that information is a common resource to be freely exchanged	All
Information is an important Trust asset. Much of the information held is available to individual members of the public under the terms of the Freedom of Information Act, subject to specific limitations and exemptions, in particular: • personal data, which can only be disclosed to the person it relates to, unless there is consent or a legal requirement • information held in confidence • credit cards details, which must not be disclosed nor stored on paper, on computer systems or audio tape All information, whether disclosable or not, must be protected from accidental or malicious loss and damage. Personal and confidential information must be protected from unintended access and disclosure and may only be disclosed to persons who can show they have a right to it.	All employees and volunteers
Every personal data set routinely shared with an external agency must be the subject of a sharing agreement based on the corporate model adapted to the particular circumstances and the nature of the information to be shared. Each agreement will define the method of transmission and the security measures that will be employed to ensure the safe	Managers

delivery of the information. ICT can advise on the various methods of secure data transmission available**.** Responsible managers will rigorously enforce agreed security measures.	
Where there are formal data-sharing agreements with other organisations, managers must ensure that all staff are aware of the existence of any such agreements, and of their terms and scope.	Managers
Personal data should not be accessed or viewed without legitimate reason. Under no circumstances will personal data held by the Trust be accessed, viewed or used for any private purpose.	All employees, visitors and contractors
Personal data should be stored on shared network drives and not on a PC"s C: drive. If the computer is "stand-alone" (not linked to a network), any essential data must be regularly copied onto alternative secure storage. Encrypted data sticks are available from the ICT helpdesk.	All
No personal data should be held on laptop computers or portable storage devices (e.g. data sticks, mobile phones) for longer than necessary to carry out intended tasks, i.e. it should be deleted after use or transferred to network storage. Staff should ensure they are registered to use laptop encryption if they carry personal or confidential data routinely. No encryption or password facility should be used other than as specified by ICT.	All
Personal data transferred to a shared portable device must be removed before the device is made available to another person.	All
Personal and confidential information in paper files or on removable media must be stored away at all times when not in use.	All
Electronic transmission of personal or confidential data should be via one of the secure email systems within the Trust.	All
Staff responsible for Trust PCs and laptops not permanently connected to the network are also responsible for regular back-up of data and for arranging for software patches to be applied and anti-virus and anti-spyware software to be regularly updated.	Managers, all employees, visitors and contractors
Documents containing personal or confidential information must be disposed of by shredding. This can be by services, through the confidential waste collection service offered by Document Solutions, or by an agency which can guarantee secure destruction. Paper containing personal data must not be recycled or used as	Managers, all employees, visitors and contractors

scrap.	
Documents, media, redundant PCs and similar equipment for disposal should be stored in a secure area until removed for disposal.	ICT
PCs, laptops and other devices must be disposed of through ICT, which will ensure all personal data has been securely removed using specialist software. If PCs are to be re-allocated then ICT will rebuild the machine in order to ensure secure deletion of any existing local data.	ICT
Data on disposable electronic media such as CDs and floppy discs, and any unwanted media containing personal data must be physically destroyed when no longer required, with due regard for personal safety, preferably using an appropriately designed shredder.	Managers, all employees,
Any loss or damage to information, or equipment that may give access to information (e.g. ID cards, tokens, laptops, mobile phones USB sticks) must be reported as soon as practicable to the Trust Operations Officer	Managers, all employees,
Any paper records taken out of the office must be treated with care, and extra care must be taken when destroying or disposing of anything outside a Trust location (e.g. at home or at a partner site).	All

Physical Security	**Responsibility**
All Trust premises other than recognised public areas are “controlled areas" for the purposes of implementing security policy.	Managers
Managers should be satisfied that access to the areas for which they are responsible is adequately controlled by their own or shared physical barriers or reception points.	Managers
Windows and doors allowing entry from uncontrolled areas must be closed and locked against external access when the location is unoccupied.	Managers, all employees,
Visitors must be identified and supervised while inside controlled areas.	Managers, all employees,
Staff should not allow unknown and unidentified persons access to any controlled area, e.g. by holding doors open. Anyone who feels unable to challenge a stranger should notify their manager or security without delay.	All employees,

Computer screens should be positioned so they are not visible from outside the immediate work area	Managers, all employees,
All staff must be alert to personal and confidential information in any form being visible beyond the immediate work area.	All employees,
CCTV systems, where installed, must be the responsibility of a nominated person who will restrict access to recordings and ensure compliance with good practice	Trust Siite Manager
All staff must be aware of the possibility of bomb threats and premises managers must be aware of the procedure to follow. Public areas should be kept tidy so that objects out of place can be identified.	All employees,

Computer Security	**Responsibility**
Every user of a system should have their own user name and a set of rights appropriate to their work.	ICT, system owners
Access to all computer applications must be controlled and protected by secure passwords.	ICT, system owners
No external party, supplier, bureau, service provider or other agency may be given access to systems, data, hardware or networks unless an appropriate access agreement has been signed by them to ensure they understand their responsibilities.	ICT, system owners
Laptops and device must be fitted with adequate protect to mitigate against cyber attacks	ICT, system owners
Passwords used to protect computer systems: • must be a minimum of 8 characters and include uppercase, lowercase and numeric characters • must not consist of purely dictionary words, personal names or words that have associations with individual users • must be changed regularly, or as required by particular systems • must not be shared with any other person • must not be written down in a manner discoverable by any other person	All employees, Members, Trustees and Governors
Computers should be logged out or the screens locked when left unattended. A 4 digit PIN should be set on all mobile phones and PDAs and the device should lock automatically after a short period of inactivity.	All employees, ICT

All staff using mobile equipment, i.e. laptops and smartphones must be aware of the additional and significant risks of: • theft (including theft from Trust premises) • loss of equipment • information "leakage" through being overlooked or overheard or interception • the opportunity for hacking presented by Bluetooth or Wi-Fi	All employees,
All staff taking information and equipment out of Trust premises should: • be aware of who is around when they use them • place Trust property away out of sight when not in use • not use Bluetooth on mobile phones and laptops • if possible use a direct cable or encrypted power line adaptor to connect to a network provider • use VPN to connect to the Trust network before surfing the internet • turn off Wi-Fi on return to the office and before connecting directly to the Trust's network.	All employees
Working at home must be carried out with similar consideration for security as office-based working. Staff transferring personal data from Trust sources to their own computer, data stick or mobile phone etc are personally liable for the legal consequences. Encryption should be enabled for staff working in a mobile setting on Trust equipment to protect personal and confidential information wherever possible	All employees
Staff who choose to use their own home computers for ad hoc work purposes must ensure that: • they have gained the agreement of their manager • they are not in breach of any formal data handling procedures which forbid use of personal equipment • the operating system and application software are patched regularly and that anti-virus, anti-spyware, and personal firewalls are installed and up to date • family members are not able to view data • data is transferred and deleted securely at the end of a working session	All employees, are responsible for ensuring these standards are met on their own computers.

Emails that are obviously spam should not be opened, but sent to the ICT team	All
Unexpected and unsolicited attachments to emails should not be opened and similar links to websites should not be followed.	All
No software should be installed or executed on a Trust owned computer without the agreement and assistance of ICT.	All employees, visitors and contractors
No hardware should be installed or attached to the Trust network without the agreement and assistance of ICT. This includes Bluetooth and Wi-Fi adapters, personal laptops, Ipods, personal cameras etc	All employees, visitors and contractors
Live personal data must not be used in the development of new computer applications, and may only be used in testing to verify consistency of output between an old system and its replacement or to assist in the resolution of an ongoing issue when all other options have been exhausted.	ICT, system owners
Anyone becoming aware of an incident or event that could compromise the security of their computer should report it to the Trust ICT team. Incidents must be also reported to the ICT team and to the Trust Operations Officer. Such incidents include, but are not limited, to: • the presence of intruders • exterior doors and windows left open inappropriately • unauthorised access or attempted access to computer systems • unauthorised access to personal data in any medium • accidental loss or disclosure of personal data • presence of a computer virus or spyware • equipment confiscated or inspected. You can raise concerns in confidence under the Whistleblowing policy.	All employees, visitors and contractors