The Diocese of Westminster Academy Trust

Information Security Policy

The Diocese of Westminster Academy Trust

Information Security Policy for the Trust

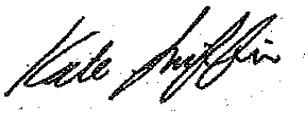
Statement of intent

The Diocese of Westminster Academy Trust is committed to maintaining the confidentiality of its information and ensuring that all information held within its schools is only accessible by the appropriate individuals. In line with the requirements of the GDPR, the Trust and its schools also has a responsibility to ensure the security of the information that is held.

The Trust has created this policy to outline how information is stored, accessed, monitored, retained, and disposed of, in order to meet the school's statutory requirements.

This document complies with the requirements set out in the GDPR, which is effective of 25 May 2018.

Signed by:



Mrs.K.Griffin
Chair of the Strategic Board
Formally agreed 28.6.18 by Trust Board

Dr.K.Sullivan
Trust DPO

The Diocese of Westminster Academy Trust

1. Introduction

1.1 All information held by the Trust in all formats, represents an extremely valuable asset and, therefore, must be used and stored in a secure manner.

1.2 This Policy is in two parts, the first outlines security procedures covering all aspects of processing information. The second part covers security of IT systems.

1.3 The Policy must be read in conjunction with other Information Management and IT Policies, including:

GDPR Data Policy, E-Safety Policy, Surveillance and CCTV Policy and Records Management Policy

1.4 The Policy applies to all Trustees, employees and volunteers of theTrust, both permanent and temporary. It also applies to contractors, business partners and visitors, not employed by the Trust but engaged to work with or who have access to the Trust information, (e.g. computer maintenance contractors) and in respect of any externally hosted computer systems.

1.5 The Policy applies to all locations from which the Trust systems are accessed (including home use). Where there are links to enable non-Trust organisations to have access to the Trust information, officers must confirm the security policies they operate meet the Trust's security requirements. A copy of any relevant third party security policy should be obtained and retained with the contract or agreement.

1.6 Suitable third party processing agreements must be in place before any third party is allowed access to personal information for which the Trust is responsible.

2 Policy Compliance

2.1 Headteachers at each of the Trust schools should ensure all staff are aware of and understand the content of this policy.

2.2 If any user is found to have breached this policy, they could be subject to the Trusts Disciplinary and Dismissal Policy & Procedure. Serious breaches of this policy could be regarded as gross misconduct.

3 Legal Aspects

3.1 Some aspects of information security are governed by legislation, the most notable UK Acts and European legislation are listed below. Further information on each can be found in Appendix 2:

- GDPR May 2018
- The Data Protection Act (1998)
- Copyright, Designs and Patents Act (1988)
- Computer Misuse Act (1990)

4 Responsibilities

4.1 All staff with management responsibilities must:

- be aware of information or portable ICT equipment which is removed from the Trust sites for the purpose of school visits or home working and ensure staff are aware of the security requirements detailed in section 9, below

- ensure all staff, whether permanent or temporary, are instructed in their security responsibilities

- ensure staff using computer systems/media are trained in their use

- determine which individuals are given authority to access specific information systems. The level of access to specific systems should be on a job function need, irrespective of status

- ensure staff are unable to gain unauthorised access to the Trust schools' IT systems or manual data

- implement procedures to minimise the Trust's exposure to fraud, theft or disruption of its systems such as segregation of duties, dual control, peer review or staff rotation in critical susceptible areas

- ensure current documentation is maintained for all critical job functions to ensure continuity in the event of relevant staff being unavailable

- ensure that the relevant system adminstrators are advised immediately about staff changes affecting computer access (e.g. job function changes leaving business unit or organisation) so that passwords may be withdrawn or changed as appropriate

- ensure that all contractors undertaking work for the Trust or its schools have signed confidentiality (non-disclosure) undertakings

- ensure the Trust's Clear Desk Policy is enforced, particularly in relation to confidential or personal information. The Clear Desk Policy can be found in Section 12 below.

- Ensure all relevant staff are aware of and comply with any restrictions specific to their role or service area. This would include, for example, Memoranda of Understanding with Government Departments, Data Sharing Agreements to which the Trust is a signatory and the Acceptable Usage Policy.

4.2 Directors, Governors and Staff are responsible for:

- ensuring that no breaches of information security result from their actions

- reporting any breach, or suspected breach of security without delay

4.3 ensuring information they have access to remains secure. The level of security will depend on the sensitivity of the information and any risks which may arise from its loss. Ensuring they are aware of and comply with any restrictions specific to their role or service area. All staff should be aware of the confidentiality clauses in their contract of employment.

4.4 Advice and guidance on information security can be provided by the Trust DPO and Academy Data Protection Lead in each school in the Trust

5 PART 1 - KEEPING INFORMATION SECURE

6 Privacy by Design

6.1 Privacy by design is an approach to projects that promotes privacy and data protection compliance from the start. The General Data Protection Regulations (GDPR), introduce a legal requirement for privacy impact assessments and privacy by design in certain circumstances.

6.2 The Trust will, therefore, ensure that privacy and data protection is a key consideration in the early stages of any project, and then throughout its lifecycle.
Such projects would include:

- A new IT system for storing and accessing personal information
- A new data sharing initiative
- A proposal to identify people in a particular group or demographic and initiate a course of action
- Using existing data for a new and unexpected or more intrusive purpose
- Introduction of a new surveillance system (CCTV) or the application of new technology to an existing system (for example adding ANPR capabilities to existing CCTV)

6.3 Core privacy considerations should be incorporated into existing project management and risk management methodologies and policies to ensure:

- Potential problems are identified at an early stage
- Increased awareness of privacy and data protection
- Legal obligations are met and data breaches are minimised
- Actions are less likely to be privacy intrusive and have a negative impact on individuals

6.4 Privacy Impact Assessments (PIAs) are an integral part of taking a privacy by design approach.

7 Data Breaches and Information Security Incidents

7.1 The Trust has a duty to ensure that all personal information is processed in compliance with the principles set out in GDPR. It is ultimately the responsibility of each Headteacher to ensure that their school complies with that duty and that suitable procedures are in place for staff to follow when dealing with personal information.

7.2 A data breach could be defined as the unintentional release of personal or sensitive personal information to an unauthorised person, either through accidental disclosure or loss/theft. However, non-compliance with any of the GDPR Data Protection Principles could be classed as a breach, particularly if there is a possibility that the students could be put at risk or suffer substantial damage or distress.

7.3 A security incident is defined as a breach of the Trust security which may result in a risk of loss, access to or corruption of the Trusts information or assets, whether personal or not.

Examples of data breaches and security incidents, including the reporting process, can be found at Appendix 1.

7.4 In the event of any breach or security incident, it is vital that action is taken to minimise any associated risk to either the Trust or its stakeholders as soon as possible.

7.5 It is important that all staff are aware of their responsibilities when handling personal information, keeping it secure and not disclosing it without proper cause. Suitable information handling procedures should be in place and all staff must undertake mandatory GDPR training on an annual basis.

7.6 Similarly, staff must be alert to the possibility of cyber-attacks or phishing attempts. Further information on cyber security can be found at Appendix 4.

7.7 In order to keep the Trust Board informed it is agreed that serious breaches involving personal information, will be reported to the next available meeting of the Risk Management Committee. The Committee will also receive a copy of the DPO's investigation into the breach.

8 Access control

8.1 Staff, Members and contractors should only access systems for which they are authorised. Under the Computer Misuse Act (1990) it is a criminal offence to attempt to gain access to computer information and systems for which they have no authorisation. All contracts of employment and conditions of contract for contractors should have a non-disclosure clause, which means that in the event of accidental unauthorised access to information (whether electronic or manual), the member of staff or contractor is prevented from disclosing information which they had no right to obtain.

8.2 Formal procedures will be used to control access to systems. An authorised manager must request each application for access and an Acceptable Use Agreement must have been signed. Access privileges will be modified/removed - as appropriate - when an individual changes job or leaves. Staff with management responsibilities must ensure they advise IT of any changes requiring such modification/removal.

8.3 Staff, Members and contractors must comply with the Trusts policy in relation to passwords.

8.4 When a member of staff leaves the employment of the Trust a leaver's form must be completed the Headteacher will ensure relevant teams are informed and access to the Trust school's network, email and buildings is removed.

8.5 In addition to the above, line managers must ensure that passwords to local systems are removed or changed to deny access. This would apply where, for example, the system is externally hosted and not under the remit of IT

8.6 Where appropriate, staff working out notice are assigned to non-sensitive tasks or are appropriately monitored.

8.7 Particular attention should be paid to the return of items which may allow future access. These include personal identification devices, access cards, keys, passes, manuals & documents.

8.8 The timing of the above requirements will depend upon the reason for the termination, and the relationship with the employee. Where the termination is mutually amicable, the removal of such things as passwords and personal identification devices may be left to the last day of employment.

8.9 Once an employee has left, it can be impossible to enforce security disciplines, even through legal process. Many cases of unauthorised access into systems and premises can be traced back to information given out by former employees.

8.10 System administrators will delete or disable all identification codes and passwords relating to members of staff who leave the employment of the Trust on their last working day. The employee's manager should ensure that all PC files of continuing interest to the business of the Trust are transferred to another user before the member of staff leaves.

8.11 Prior to a member of staff leaving, it is good practice for a meeting to be held during which the manager notes all the systems to which the member of staff had access and informs the relevant system administrators of the leaving date. Special care needs to be taken when access to personal, commercially sensitive or financial data is involved.

8.12 Managers must ensure that staff leaving the Trust's employment do not inappropriately wipe or delete information from hard disks. If the circumstances of leaving make this likely then access rights should be restricted to avoid damage to the Trusts information and equipment.

8.13 All visitors should have official identification issued by the Trust school they are visiting. If temporary passwords need to be issued to allow access to confidential systems these need to be disabled when the visitor has left. Visitors should not be afforded an opportunity to casually view computer screens or printed documents produced by any information system without authorisation.

8.14 There is a requirement for system administrators to have a procedure in place for the secure control of contractors called upon to maintain and support computing equipment and software. The contractor may be on site or working remotely via a communications link. The IT Managers in each Trust school will advise on the most suitable control.

8.15 Physical security to all office areas should be maintained. Staff should challenge strangers in the office areas without an ID badge. Never let someone you don't know or recognise to tailgate you through security doors.

9 Security of Equipment

9.1 Portable computers must have appropriate access protection, for example passwords and encryption, and must not be left unattended in public places.

9.2 Computer equipment is vulnerable to theft, loss or unauthorised access. Always secure laptops and handheld equipment when leaving an office unattended and lock equipment away when you are leaving the office.

9.3 Due to the high incidence of car thefts laptops or other portable equipment must **never** be left unattended in cars or taken into vulnerable areas.

9.4 Users of portable computing equipment are responsible for the security of the hardware and the information it holds at all times on or off Trust property. The equipment should only be used by the individual to which it is issued, be maintained and batteries recharged regularly.

9.5 Staff working from home must ensure appropriate security is in place to protect Trust equipment or information. This will include physical security measures to prevent unauthorised entry to the home and ensuring Trust equipment and information is kept out of sight.

9.6 Trust issued equipment must not be used by non-Trust staff.

9.7 All of the policy statements regarding the use of software and games apply equally to users of portable equipment belonging to the Trust.

9.8 Users of this equipment must pay particular attention to the protection of personal data and commercially sensitive data. The use of a password to start work with the computer when it is switched on, known as a 'power on' password, is mandatory and all sensitive files must be password protected if encrypting the data is not technically possible. The new user will refer to the instruction book to learn how to apply these passwords or may make arrangements for basic training in the use of a portable computer.

9.9 Users of portable equipment away from Trust premises should check their car and home insurance policies for their level of cover in the event of equipment

being stolen or damaged and take appropriate precautions to minimise risk of theft or damage.

9.10 Staff and Members who use portable computers belonging to the Trust must use them solely for business purposes otherwise there may be a personal tax/National Insurance liability.

10 Security and Storage of Information

10.1 All information, whether electronic or manual, must be stored in a secure manner, appropriate to its sensitivity. It is for each service area to determine the sensitivity of the information held and the relevant storage appropriate to that information. Suitable storage and security will include:

- Paper files stored in lockable cupboards or drawers
- Laptops stored in lockable cupboards or drawers
- Electronic files password protected or encrypted
- Restricted access to ICT systems
- Computer screens to be 'locked' whenever staff leave their desk
- Removable media to be kept in lockable cupboards or drawers and information deleted when no longer required
- Paper files removed from the office (for school visits or when working from home) to be kept secure at all times and not left in plain sight in unattended vehicles or premises
- Laptops must **never** be left in unattended vehicles
- It is advisable that paper files containing personal or sensitive data are kept separate from laptops, particularly when working from home
- At no time should sensitive, confidential or personal information be stored on a portable unit's hard drive. Access to this type of information must always be through the Trust school's network.
- To preserve the integrity of data, frequent transfers must be maintained between portable units and the main Trust schools computer system.
- Staff should be aware of the position of their computer screens and take all necessary steps to prevent members of the public or visitors from being able to view the content of computers or hard copy information

11 Clear Desk Policy

11.1 Employees are required to clear working documents, open files, and other paperwork from their desks, working surfaces and shelves at the end of each working day and to place them securely into desk drawers and cupboards as appropriate.

11.2 Although security measures are in place to ensure only authorised access to office areas, employees should ensure that documents, particularly of a confidential nature are not left lying around.

11.3 Employees must ensure that documents are carefully stored. When properly implemented, this clear desk policy also improves efficiency as documents can be retrieved more easily.

12 Posting, Emailing or Faxing Information

12.1 If information is particularly sensitive or confidential the most secure method of transmission must be selected. The following procedures should be adopted as appropriate, depending on the sensitivity of the information.

12.2 Please consider the risk of harm or distress that could be caused to the stakeholder if the information was lost or sent to another person, then look at the most appropriate way of sending the information to the recipient.

12.3 It is important that only the minimum amount of personal or sensitive information is sent, by whichever method is chosen.

12.4 Sending information by fax:

- telephone ahead to advise the fax is being sent and ask for confirmation of receipt
- Check the fax number is correct and dial carefully
- If the information is particularly sensitive, send a test fax to ensure it reaches the correct recipient
- Always use a fax header sheet, providing contact details of the sender and recipient

12.5 Sending information by email:

- Carefully check the recipient's email address before pressing send – this is particularly important where the 'to' field autocompletes
- If personal or sensitive information is regularly sent via email, consider disabling the auto complete function and regularly empty the auto complete list. Both of these options can be found in Outlook under 'file', 'options' and 'mail'
- Take care when replying 'to all' – do you know who all recipients are and do they all need to receive the information you are sending
- If emailing sensitive information, password protect any attachments. Use a different method to communicate the password eg telephone call, messenger or text.
- Consider the use of secure email where this is available

- Person identifiable data files **must not** be sent via email to a user's personal mail box. Staff working from home should only access information via the Trust school's network.

12.6 Sending information by post:

- Check that the address is correct
- Ensure only the relevant information is in the envelope and that someone else's letter hasn't been included in error
- If the information is particularly sensitive or confidential, discuss the most secure method of delivery with the Post room, this could be by Recorded, Special Delivery or even courier.

12.7 Printing and Photocopying:

- All printing must be via the Trust printers
- Consideration must be given to using a confidential copier to print or large print runs, especially where personal information is concerned
- When printing or photocopying multiple documents, ensure you separate them when you return to your desk
- If the copier jams please remove all documents – if the copier remains jammed report it, but leave your contact details on the copier so that once it has been fixed any remaining copying can be returned to you. If possible, cancel your print run
- Make sure your entire document has copied or printed – check that the copier has not run out of paper. This is particularly important when copying or printing large documents. Please bear in mind the printer will sometimes pause in the middle of a large print run
- Do not leave the printer unattended when you're using it – someone else may come along and pick up your printing by mistake

13 Redacting

13.1 If it is necessary to redact information, either before sending it out or posting it onto the website, ensure a suitable and permanent redaction method is used

13.2 The use of black marker pen is **not** a suitable method of redaction

13.3 It is not advisable to change the colour of text (eg white text on a white background) or use text boxes to cover text as these can be removed from electronic documents. However, if this is the only option, once redacted the document should be printed and then scanned as a PDF before being sent.

14 Sharing and Disclosing Information

14.1 When disclosing personal or sensitive information to stakeholders, particularly over the phone or in person, ensure you verify their identity. If in doubt ask for suitable ID or offer to post the information (to the contact details you have on file)

14.2 If a request for disclosure of information is received from a third party, you must:

- Obtain written consent from the customer that they are acting on their behalf
- verify their identity, particularly if they request information via the telephone or in person. It is preferable to telephone the person back, using a recognised telephone number for their organisation (for example 101 for the Police). Do not take their mobile number and use that.

14.3 In all circumstances, you must ensure you are legally able to share the information being requested and only share the minimum amount of information necessary.

15 Retention and Disposal of Information

15.1 Information must only be retained for as long as it is needed for business purposes, or in accordance with any statutory retention period

15.2 Staff should refer to the Trusts Retention of Records Policy.

15.3 When disposing of information please ensure the most appropriate method is used. Paper files containing personal or sensitive information must be disposed of in the confidential waste bins. Electronic information must be permanently destroyed

15.4 When purchasing new computer systems or software, please consider requirements for the retention and disposal of information and ensure these are included at the scoping stage

16 Vacating Premises or Disposing of Equipment

16.1 It is important that a process is in place to ensure all Trust information is removed from premises should they be vacated and from equipment before it is disposed of. Equipment includes cupboards and filing cabinets as well as computers or other electronic devices.

16.2 The disposal of computer or other electronic devices is referenced in this policy and all electronic equipment must be returned to the IT Team to be properly disposed of.

17 PART 2 – ICT SECURITY

18 Cloud Storage Solutions

18.1 The use of cloud storage solutions (Skydrive, Onedrive Personal, iCloud etc.) for the transfer of Trust information is expressly forbidden. The IT Team at each Trust school can provide you with access to its secure process for the sharing of files.

19 Systems Development

19.1 All system developments must comply with the Trust schools ICT Strategy. All system developments must include security issues in their consideration of new developments, seeking guidance from the IT Manager, where appropriate the Trust Board depending on the contract size.

19.2 Privacy Impact Assessments (PIAs) should be carried out prior to the purchase of any new system which will be used for storing and accessing personal information.

20 Network Security

20.1 The Trust may engage a third-party specialist to routinely review network security.

21 Risks from Viruses

21.1 Viruses (including malware and zero day threats) are one of the greatest threats to the Trust's computer systems. PC viruses become easier to avoid with staff and members aware of the risks with unlicensed software or bringing data/software from outside the Trust. Anti-virus measures reduce the risks of damage to the network.

21.2 IT Teams at each Trust school centrally maintain and update the currency of the virus definition files on servers, but users are responsible for checking that virus updates are automatically occurring on all desktop machines. Any concerns please discuss with your IT Team immediately.

22 Cyber Security

22.1 Cyber security and cybercrime are increasing risks that, if left unchecked, could disrupt the day to day operations of the Trust,ultimately have the potential to compromise national security.

22.2 The Trust's approach to cyber security can be found in Appendix .

23 Access Control to Secure Areas

23.1 Secure areas include:

- School Offices- holding school files and records
- The ICT server room in each Trust school

All central processors/networked file servers/central network equipment will be located in secure areas with restricted access.

Local network equipment/file servers and network equipment will be located in secure areas and where appropriate within locked cabinets.

Unrestricted access to the computer facilities will be confined to designated staff whose job function requires access to that particular area/equipment.

Restricted access may be given to other staff where there is a specific job function need for such access.

Authenticated representatives of third party support agencies will only be given access through specific authorisation.

All secure areas will have an entry log which staff and visitors must use.

Regular reviews of who can access these secure areas should be undertaken.

24 Security of Third Party Access

24.1 No external agency will be given access to any of the Trust's networks unless that body has been formally authorised to have access.

24.2 All external agencies will be required to sign security and confidentiality agreements with the Trust.

24.3 All external agencies processing personal information on the Trust's behalf (including via a hosted IT system) will be required to sign a third party processing agreement.

24.4 The Trust will put in place adequate policies and procedures to ensure the protection of all information being sent to external systems. In doing so, it will make no assumptions as to the quality of security used by any third party but will request confirmation of levels of security maintained by those third parties. Where levels of security are found to be inadequate, alternative ways of sending data will be used.

24.6 All third parties and any outsourced operations will be liable to the same level of confidentiality as Trust Staff.

25 Data Back-up

25.1 Data should be held on a network directory where possible, to ensure routine backup processes capture the data. Information must not be held on a PC hard drive without the approval of the IT Manager.

25.2 Data should be protected by clearly defined and controlled back-up procedures which will generate data for archiving and contingency recovery purposes.

25.3 IT Services and all other systems administrators should produce written backup instructions for each system under their management. The backup copies should be clearly labelled and held in a secure area. Procedures should be in place to recover to a useable point after restart of this back-up. A cyclical system, whereby several generations of backup are kept, is recommended.

25.4 Archived and recovery data should be accorded the same security as live data and should be held separately preferably at an off-site location. Archived data is information which is no longer in current use, but may be required in the future, for example, for legal reasons or audit purposes. The Trust's Retention Schedule must be followed in determining whether data should be archived.

25.5 Recovery data should be sufficient to provide an adequate level of service and recovery time in the event of an emergency and should be regularly tested.

25.6 To ensure that, in an emergency, the back-up data is sufficient and accurate, it should be regularly tested. This can be done by automatically comparing it with the live data immediately after the back-up is taken and by using the back-up data in regular tests of the contingency plan.

25.7 Recovery data should be used only with the formal permission of the data owner or as defined in the documented contingency plan for the system.

25.8 If live data is corrupted, any relevant software, hardware and communications facilities should be checked before using the back-up data. This aims to ensure that back-up data is not corrupted in addition to the live data. An engineer (software or hardware) should check the relevant equipment or software using his/her own test data.

26 Equipment, Media and Data Disposal

26.1 If a machine has ever been used to process personal data as defined under GDPR or 'in confidence' data, then any storage media should be disposed of only after reliable precautions to destroy the data have been taken. Procedures for disposal should be documented.

26.2 Many software packages have routines built into them which write data to temporary files on the hard disk for their own purposes. Users are often unaware that this activity is taking place and may not realise that data which may be sensitive is being stored automatically on their hard disk.

26.3 Although the software usually (but not always) deletes these files after they have served their purpose, they could be restored and retrieved easily from the disk by using commonly available utility software. Therefore, disposal must be arranged through the IT Team at the Trust school who will arrange for disks to be wiped or destroyed to the appropriate standards.

27 Software

27.1 All users should ensure that they only use licensed copies of commercial software. It is a criminal offence to make/use unauthorised copies of commercial software and offenders are liable to disciplinary action. Each user should ensure that a copy of each licence for commercial software is held.

27.2 The loading and use of unlicensed software on Trust computing equipment is **NOT** allowed. All staff and members must comply with the Copyright, Designs and Patents Act (1988). This states that it is illegal to copy and use software without the copyright owner's consent or the appropriate licence to prove the software was legally acquired. 28.3 The Trust will only permit authorised software to be installed on its PCs. Approval will be via IT Services.

27.4 Where the Trust recognises the need for specific specialised PC products, such products should be registered with IT Services and be fully licensed.

27.5 Software packages must comply with and not compromise the Trusts security standards.

27.6 Computers owned by the Trust are only to be used for the work of the Trust. The copying of leisure software on to computing equipment owned by the Trust is not allowed. Copying of leisure software may result in disciplinary action under the Trust's Disciplinary and Dismissal Policy & Procedure. Computer leisure software is one of the main sources of software corruption and viruses which may lead to the destruction of complete systems and the data contained on them.

27.7 Educational software for training and instruction should be authorised, properly purchased, virus checked and loaded by the IT Team at the Trust school or its authorised representatives. Where a software training package includes 'games' to enable the new user to practise their keyboard skills e.g. Windows, then this will be allowed as long as it does not represent a threat to the security of the system.

27.8 The Trust seeks to minimise the risks of computer viruses through education, good practice/procedures and anti-virus software positioned in the most vulnerable areas. Users should report any viruses detected/suspected on their machines immediately to the Trust schools IT Team.

27.9 Users must be aware of the risk of viruses from email and the internet. If in doubt about any data received please contact IT Services for anti-virus advice.

28 Use of Removable Media

28.1 It is the Trust's policy to prohibit the use of all unauthorised removable media devices. The use of removable media devices will only be approved if a valid business case for its use is developed.

28.2 All staff, Members and third parties must comply with the requirements regarding removable media.

29 Timeout Procedures

29.1 Inactive computers should be set to time out after a pre-set period of inactivity. The time-out facility should clear the screen. In high risk areas the time-out facility should also close both application and network sessions. A high risk area might be a public area .The time-out delay should reflect the security risks of the area.

29.2 Users must 'lock' their computers, if leaving them unattended for any length of time. For high risk applications, connection time restriction should be considered. Limiting the period during which the computer has access to IT services reduces the window of opportunity for unauthorised access.

30 System Documentation

30.1 All systems should be adequately documented by the IT Team and should be kept up to date so that it matches the state of the system at all times.

30.2 System documentation, including manuals, should be physically secured (for example, under lock and key) when not in use. An additional copy should be stored in a separate location which will remain secure, even if the computer system and all other copies are destroyed.

31.5 General Internet access carries with it a security risk of downloading viruses or programs that can look around a network and infiltrate password security systems. This information can then be sent back to the originator of the program in order to allow them unauthorised access to our systems. Therefore care must be taken when transferring data between your home PC and the Trust network. All home PCs which are used for the manipulation of Trust data must have a current virus checker with up to date virus signatures.

APPENDIX - Anti-Virus Guidelines

1. What is a virus?

A computer virus is a damaging piece of software that can be transferred between programs or between computers without the knowledge of the user. When the virus software is activated (by incorporated instructions, e.g. on a particular date), it performs a range of actions such as displaying a message, corrupting software, files and data to make them unusable, and deleting files and/or data. While many of the viruses produced are benign and cause no real damage to the infected system, they always constitute a breach of security.

There are currently something like 60-75,000 known viruses and worms [1] - some 10-20 new viruses or variants appear a day. When a virus or worm is released into the public domain, network worms and mass mailer viruses can sometimes spread worldwide before anti-virus vendors have had time to produce updates.

[1] A worm is a self-replicating virus that does not alter files but resides in active memory and duplicates itself. Worms use parts of an operating system that are automatic and usually invisible to the user. It is common for worms to be noticed only when their uncontrolled replication consumes system resources, slowing or halting other tasks.

Even daily anti-virus updates are not always enough to ensure safety from all possible threats.

2. What does the Trust's IT Services do to prevent the spread of viruses?

Whilst precautions are taken at the network level to minimise the spread and impact of worms and viruses, it is not possible to make the process totally effective. Protection from viruses and worms is not a process that can be left entirely to system administrators, security officers, and anti-virus software. The best efforts of administrators and security experts are not sufficient - all computer users must also play their part by taking simple precautions like those described below.

3. Avoid Unauthorised Software

Programs like games, joke programs, cute screensavers, unauthorised utility programs and so on can sometimes be the source of difficulties even if they are genuinely non-malicious. That is why it is forbidden to install them. If such programs are claimed to be some form of antivirus or anti-Trojan [2] utility, there is a high risk that they are actually in some way malicious!

4. Treat all attachments with caution

It makes sense to be cautious about email attachments from people you don't know. However, if attachments are sent to you by someone you do know, don't assume they must be OK because you trust the sender.

Worms generally spread by sending themselves without the knowledge of the person from whose account they spread. If you do not know the sender or are not expecting any messages from the sender about that topic, it is worth checking with the sender that they intended to send a message, and if so, whether they intended to include any attachment. If you were expecting an attachment from them, this may not apply.

However, one recent virus sends out an email telling you that a 'safe' attachment is on the way, then sends out mail with a copy of itself as an attachment.

Bear in mind that even legitimate, expected attachments can be virus infected: worms and viruses are related, but cause slightly different problems.

Regard anything that meets the following criteria with particular suspicion:

- If they come from someone you don't know, who has no legitimate reason to send them to you.
- If an attachment arrives with an empty message.
- If there is some text in the message, but it doesn't mention the attachment.

[2] In computers, a Trojan horse is a program in which malicious or harmful code is contained inside apparently harmless programming or data in such a way that it can get control and do its chosen form of damage. In one celebrated case, a Trojan horse was a program that was supposed to find and destroy computer viruses. A Trojan horse may be widely redistributed as part of a computer virus.

- If there is a message, but it doesn't seem to make sense.

- If there is a message, but it seems uncharacteristic of the sender (either in its content or in the way it's expressed).

- If it concerns unusual material like pornographic web-sites, erotic pictures and so on.

- If the message doesn't include any personal references at all, (for instance a short message that just says something like "You must take a look at this", or "I'm sending you this because I need your advice").

- If the attachment has a filename extension that indicates a program file (such as those listed below).

- If it has a filename with a 'double extension', like FILENAME.JPG.vbs or FILENAME.TXT.scr, that may be extremely suspicious. As far as Windows is concerned, it's the last part of the name that counts, so check that against the list below to find out whether it's a program like those listed, masquerading as a data file, such as a text file or JPEG (graphics) file.

In all the above instances, it is recommended that you check with the sender that they knowingly sent the mail/attachment in question.

5. Avoid unnecessary macros

If Word or Excel warn you that a document you're in the process of opening contains macros [3], regard the document with particular suspicion unless you are expecting the document and you know that it's supposed to contain macros. Even then, don't enable macros if you don't need to. It may be worth checking with the person who sent it to you that it is supposed to contain macros.

6. Be cautious with encrypted files

If you receive an encrypted (passworded) attachment, it will normally be legitimate mail from someone you know, sent intentionally (though the sender is unlikely to know in the event that they have a virus). However, that doesn't necessarily mean that it isn't virus-infected. If it started out infected, encryption won't fix it. Furthermore, encrypted attachments can't usually be scanned for viruses in transit: the onus is on the recipient to be sure the decrypted file is checked before it's opened. This goes not only for heavyweight encryption packages, but also for files compressed and encrypted with PKZip or WinZip.

7. Suspicious filename extensions

The following is a list of filename extensions that indicate an executable [4] program, or a data file that can contain executable programs in the form of macros. This list is by no means all-

---

[3] In Microsoft Word and other programs, a macro is a saved sequence of commands or keyboard strokes that can be stored and then recalled with a single command or keyboard stroke. A macro virus is a computer virus that "infects" a Microsoft Word or similar application and causes a sequence of actions to be performed automatically when the application is started or something else triggers it.

[4] An executable is a file that contains a program. It is a particular kind of file that is capable of being executed or run as a program in the computer. In a Windows operating system, an executable file usually has a file name extension of .bat, .com, or .exe.

inclusive. There are probably a couple of hundred filename extensions that denote an executable program of some sort.

Furthermore, there are filenames like .RTF that shouldn't include program content, but sometimes can, while Word documents (for instance) can in principle have any filename extension, or none. Furthermore, zipped (compressed) files with the filename extension .ZIP can contain one or more of any kind of file.

.BAT	.CHM	.CMD	.COM	.DLL	.DOC	.DOT
.EXE	.FON	.HTA	.JS	.OVL	.PIF	.SCR
.SHB	.SHS	.VBS	.VBA	.WIZ	.XLA	.XLS

8. Report it!

If you think that you may have received a virus - report it!

APPENDIX - Cyber Security Approach

1. Introduction

This document identifies the risks to the Trust from main threats of cyber security and sets out what is in place to mitigate these risks.

If you do not understand anything in this document or feel you need specific training you should bring this to the attention of your line manager.

2. Purpose and Objectives

The document provides guidance to staff and members on the risks that threats from cyber security pose to the Trust.

3. Roles and Responsibilities

The IT Manager is responsible for the provision of the appropriate technology and technological devices to ensure that the Trust schools are reasonably protected from the threats from cyber security.

The Trust is responsible ensuring that staff are communicated with about how to ensure that they don't put the Trust at risk.

All Directors, governors employees and contractors should not take any action that puts the Trusts systems or information at risk from cyber security. Any incidents must be reported in line with the Information Security policy.

4. Cyber Security

Cyber security and cybercrime are persistent threats that, if left unchecked, could disrupt the day to day operations of the Trust and have the potential to compromise national security. Additional costs will be incurred by the Trust to rectify any cyber security or cybercrime event.

Technical advances create opportunities for greater efficiency and effectiveness. These include more engaging and efficient digital services, new ways to work remotely and to store and transfer data, such as mobile devices and cloud services.

The scale of targeted attacks, coupled with the difficulty of monitoring all possible attack methods requires the public sector to work together to both reduce the likelihood and the impact of such a threat succeeding.

Foreign states, criminals, hacktivists, insiders and terrorists all pose different kinds of threats. They may try to compromise public sector networks to meet various objectives that include:

- Stealing sensitive information to gain economic, diplomatic or military advantage over the UK
- Financial gain
- Attracting publicity for a political cause
- Embarrassing central and local government
- Controlling computer infrastructure to support other nefarious activity
- Disrupting or destroying computer infrastructure

Trust employees can also be targets for criminal activity.

5. Cyber Security Risks

The following types of cyber security all pose risks to the Trust:

- Cybercrime:

The most common form of cyber-attack against public bodies is the use of stolen or false customer credentials to commit fraud.

The uptake in online services means this form of crime can now be undertaken on a much larger scale and can be international.

Cybercriminals also seek to steal data from government networks that has a value on the black market, such as financial information or data that can be used for ID theft.

There are several types of malware (malicious software) that have been written to specifically steal banking and log in information.

The Trust secures its network with up to date antivirus and malware protection, and manages the use of personal USB devices on Trust computers.

- Hacktivism:

Hacktivists seek to cause embarrassment or annoyance to the owners of high profile websites and social media platforms that they may deface or take off line.

When targeted against public services websites and networks, these attacks can cause reputational harm both locally and nationally.

The Trust's web site's content management system conforms to the Trusts GDPR Policy with regards to password enforcement.

- Insider threats:

An insider is someone who exploits, or intends to exploit, their legitimate access to an organisation's assets for unauthorised purposes. Such activity can include:

- Unauthorised disclosure of sensitive information
- Facilitation of third party access to an organisation's assets
- Physical sabotage
- Electronic or IT sabotage

Not all insiders deliberately set out to betray their organisation. An unwitting insider may compromise their organisation through poor judgment or due to a lack of understanding of security procedures.

The insider threat is not new, but the environment in which insiders operate has changed significantly. Technology advances have created opportunities for staff at all levels to access information.

The Trust enforces the use of strong passwords for access to systems.

The Trust only allows corporate USB devices to be written to. All personal USB devices are read only.

The Trust uses mobile device management tools to secure corporate information on personal devices (smart phones and tablets).

The Trust periodically reviews access to key IT systems.

- Physical Threats:

The increasing reliance on digital services brings with it an increased vulnerability in the event of a fire, flood, power cut or other disaster natural or otherwise that could impact upon the Trusts IT systems.

The Trust schools have a disaster recovery (DR) and business continuity (BC) data centre for its high impact services

- Terrorists:

Some terrorist groups demonstrate intent to conduct cyber-attacks, but have limited technical capability. Terrorist groups could acquire improved capability in a number of ways, namely through the sharing of expertise in online forums providing an opportunity for escalations and the hiring of Hacktivists.

6. The Trust's approach to Cyber Security

As with most Academy Trusts we rely heavily on access to the internet and to information held in its systems. There are several IT systems that have an internet presence (website, webmail homeworking), and there are several different access mechanisms to information (Wi-Fi, physical networking, smartphones, tablets). All present threats to cyber security. It is widely

acknowledged that it is not currently possible to keep out all attacks all of the time, but the Trust employs a range of tools and good practice to minimise the risk to its information and systems.

The Trust has clear polices on ICT and Information Security, which provide information on a range of areas including:

- Reporting of security incidents
- Use and security of emails
- Use of the internet
- Mobile phone usage
- Passwords
- Removable Media
- Clear desk policy
- Sharing and disclosing information
- Cloud storage systems
- Viruses
- Equipment, media and data disposal

The Trust employs a range of technology and processes to help it achieve a good security platform. These range from up to date firewalls and core networking equipment, through antivirus controls and a secure wireless configuration and to encrypted devices.