The Midland Academies Trust

Information Technology Security Policy 2018

The Midland Academies Trust

Group Director E-Services

HARTSHILL • SCHOOL

the Nuneaton Academy

The George Eliot School

Heath Lane Academy

Approval Date: Summer 2018

Next Approval: Summer 2021

Contents

Information Technology Security Policy 2018

1. Introduction

1.1. The ease with which data can be accessed, passed within and external to the Trust, often by computer, is an undoubted benefit for employees involved in the delivery of services. All those concerned need to be aware that there is a legal duty to protect the security of Trust's IT systems and the confidentiality of Trust information. Stakeholders have the right to respect for their privacy, and hence an expectation that information about them will be treated as confidential.

1.2. This IT Security Policy is based on that expectation, but also acknowledges that Trust employees will need to have controlled access to student, financial and staff information to ensure that the Trust functions effectively, efficiently and in a safe manner.

2. Definitions

2.1 "Use" is anyone who uses Trust hardware or software or systems.

2.2 "Trust equipment" shall be taken to mean hardware, software or any other IT related system operated by the Trust.

2.3 "Inappropriate use" shall be interpreted by the Trust Executive Principal with advice of the Group Director E-Services but shall specifically include, but not be limited to, accessing pornographic images or other content deemed offensive, the unlicensed and illegal use of software, unauthorised attempts to access secure systems, breaches of data protection and the unauthorised installation of software onto Trust equipment. Such misuse will be subject to Trust disciplinary procedures.

2.4 "Confidentiality" means ensuring that data and information is accessible only to those users authorised to have access.

2.5 "Integrity" means safeguarding the accuracy and completeness of data, information and processing methods.

2.6 "Availability" means ensuring that authorised users have access to data, information and associated assets when required.

3. Related Policies, Procedures and Documents

3.1 General Data Protection Regulation Policy

3.2 Safeguarding Policy

4. Rationale

4.1 The Trust must protect its information assets, defined for the purposes of this Policy as computers, hardware, networks, software and all of the data they contain and its reputation. This will help the Trust to:

i. Ensure that a high quality service is offered to our staff, students and other clients.

ii. Maintain and improve its reputation and meet its legal obligations and strategic business and professional goals.

iii. Prevent data loss.

iv. Prevent data breaches.

4.2 Ensure that users are aware of their personal responsibilities for protecting data in accordance with Trust or any external organisation's guidelines.

5. Core Principles

5.1 The Trust must comply with a variety of legislation in this regard, including but not limited to:

i. General Data Protection Regulation;

ii. The Human Rights Act 1998;

iii. The Computer Misuse Act 1990;

iv. The Regulation of Investigatory Powers Act 2000;

v. The Freedom of Information Act 2000;

vi. The Copyright, Designs and Patents Act 1988;

vii. The Electronic Communications Act 2000.

viii. The Counter Terrorism and Security Act 2015

5.2 Security of the Trust system will be proactively monitored and breaches of security will be reported, investigated and the cause corrected as soon as possible.

5.3 Only appropriate use will be made of Trust equipment and in particular of the data held within.

5.4 Notwithstanding the requirements of the General Data Protection Regulation, the Trust retains its right to monitor the use of its systems by any user in order to protect its legitimate business and reputation.

5.5 Appropriate internal and external systems will be employed to help the Trust ensure the security of its systems.

5.6 Due thought and consideration will be given to information security risks prior to implementation of new systems and all new systems will undergo a Data Protection Impact Assessment

6. Equality Analysis

6.1 By virtue of the provisions of the Equality Act 2010, the Trust has a duty to have due regard to the need to:

i. eliminate unlawful discrimination, harassment and victimisation and other prohibited conduct;

ii. advance equality of opportunity between people of different groups;

iii. foster good relations between people from different groups.

6.2 In implementing this Policy and associated procedures, the Trust will actively take these aims into account as part of its decision making process and will demonstrate how this has been undertaken.

6.3 Where necessary a full equality impact assessment will be undertaken.

7. Implementation, Monitoring and Review

7.1 Responsibilities

The E-Services department has responsibility for co-ordinating IT Security. Specific members of E-Services must be endowed with sufficient and appropriate authority, allowed direct access to all users and data, and be capable of establishing the effectiveness of the security procedures.

7.1.2 E-Services

i. Ensuring that IT systems in use are appropriately assessed for security compliance and are protected in accordance with the IT Security Policy. Requests for systems by internal departments will incorporate an appropriate assessment of security requirements and a Data Protection Impact Assessment

ii. Ensuring backup systems remain fit for purpose.

iii. Ensuring Anti-virus guards remain fit for purpose.

iv. Ensuring external threats are mitigated through sufficient firewall protection.

v. Ensuring appropriate levels of access are provided to users.

vi. Ensuring that the IT security standards are implemented effectively and reviewed.

7.1.3 Users

i. Comply with the Trust Information Technology Security Policy and related policies and procedures.

ii. Comply with the General Data Protection Regulation Policy.

iii. Comply with any other applicable legislation and guidelines.

iv. Notify E-Services immediately of IT security breaches which come to their attention.

v. Be proactive in supporting the security of the network, particularly in relation to students understanding of policies and procedures.

vi. Notify the Trust DPO immediately of any information breaches that come to their attention. The Trust may be required to share information with external agencies.

7.2 Remote Services

7.2.1 The Trust recognises that due to the nature of delivery, remote access to systems is valuable and at times essential to the learner experience. The Trust will aim to provide remote access to systems with due consideration to security. Not all systems are capable of operating remotely, nor should the expectation be that every system can be accessed remotely. An assessment of risk, technical capability and need would define the decision.

7.2.2 Where security information is required in order to access a remote system encryption must be implemented. E-Services will advise of and provide the necessary certification.

7.2.3 On occasion 3rd parties may require access to the Trust network e.g. to perform maintenance tasks or provide support. Users must not share access details to the 3rd party without consultation with E-Services. E-Services will define an appropriate method of access dependant on requirements for a fixed period of time.

7.3 Anti-Virus

7.3.1 The deliberate introduction of malicious software to a system is a criminal offence under the Computer Misuse Act 1990.

7.3.2 E-Services will aim to mitigate the infection of the network by proactively remaining up to date with relevant anti-virus software. Users should be proactive in contacting E-Services should they have concern with Anti-Virus software, on any device they have access to.

7.3.3 Where users suspect a virus, no files should be loaded on to any system from an external device without prior consultation with E-Services.

7.3.4 All relevant servers and most PCs have anti-virus software installed. Servers and PCs which do not have anti-virus software installed are protected by a firewall and are not accessed by usual / normal users as those PCs have a specialist infrastructure function and are not for general staff use.

7.3.5 Where a virus is detected this will be reported immediately to E-Services who will attempt to "clean" and rebuild the affected PC and update the anti-virus.

7.4 **Mobile Devices**

7.4.1 The large scale rise in the use of mobile devices and hosted services, including but not limited to, laptops, USB/Flash memory, PDAs, Smartphones, External Hard Drives, "cloud" data storage and email, social networking, presents a challenge to the security of data. In particular the unauthorised loss or release of personal or sensitive data to an external source, can have financial and legal implications.

7.4.2 The value of mobile technology can undoubtedly be harnessed to improve organisational efficiency and add value to the student experience, but usage does need to come with relevant safeguards.

7.4.3 Trust mobile phones and smartphones are provided via a central contract. Users are required to abide by the contract they sign upon receipt and to be vigilant about the usage of the device. Users should not store personal or sensitive data on these devices and use sufficient safeguards to prevent loss or theft of data (e.g. pin code). E-Services are available for advice when required. Prior to accessing data services via personal devices (i.e. not Trust owned equipment), we strongly recommend users seek advice from E-Services.

7.4.4 Laptops and other mobile devices are provided through E-Services on request, dependant on budget and compatibility.

7.4.5 Laptops are capable of holding "shadow copies" of the users own personal "home" drives. Shared folder access is through VPN or Remote Desktop only. Users must abide by Data Protection guideline and legislation when considering what to store on their allocated drives. Failure to give due consideration to the GDPR principles could result in disciplinary procedures, for example personal data of students should not be held outside of Trust provided storage mediums unless permission has been provided by E-Services and to ensure appropriate encryption methods have been employed.

7.4.6 Access to portable storage devices is only granted to specific users and/or devices with the approval of the Group Director E-Services. This includes the use of USB storage devices.

7.5 **Protection of Hardware**

7.5.1 Purchasing, maintenance and disposal of hardware must be done in conjunction with E-Services.

7.5.2 A central asset list of Trust owned equipment is held within E-Services.

7.5.3 No equipment should be removed from any site or room without the approval of E-Services, except for portable laptops or devices that are the responsibility of each named individual user or department.

7.5.4 Users will be responsible for organising PAT testing of any devices for which they have responsibility e.g. laptops. A central PAT testing service is available through the Estates department. Learners bringing in their own equipment are also required to have devices PAT tested through the Estates department.

7.5.5 Hardware in particularly vulnerable areas or containing sensitive data should make use of physical security measures such as locking office doors or installing locking devices to secure hardware to desk. Contact E-Services for further guidance.

7.5.6 Redundant hardware will be disposed of via E-Services **only,** in accordance with IEEE directives.

7.5.7 All personal computers and non-essential peripherals should be switched off when not in use for extended periods, such as overnight or during weekends, except for essential Server Room equipment or local site servers.

7.5.8 Any media storage (e.g. CD ROM/DVD) should be labelled and kept in boxes with sensitive media stored in locked desks or fireproof safes.

7.6 **Protection of Data from Hardware Loss**

7.6.1 Backups of data and system programmes will be taken on a regular basis as determined by the E-Services Manager.

7.6.2 Data should not be held locally on PCs or laptops, as this is not included in the automatic nightly backup of the network servers. Data should be saved to servers (e.g. shared folders). E-Services cannot be held responsible for loss of data that is stored on a local drive.

7.6.3 Backup recovery procedures will be tested on a regular basis as determined by the E-Services Manager.

7.6.5 The Trust Disaster Recovery plan is reviewed by the Executive Director Corporate Services.

7.7 **Protection of Data from Unauthorised Access**

7.7.1 Staff account passwords controls must be implemented. Passwords will have the following characteristics enforced:

i. be at least 8 characters long;
ii. contain letters and numbers;
iii. be different from the 15 previous passwords used;
iv. be user generated;
v. will be required to be changed every 90 days.

7.7.2 Student user accounts and passwords are created using SIMS

7.7.3 System password details are recorded by E-Services and kept securely.

7.7.4 To prevent others gaining access to network accounts care should be taken when logging in to the network to prevent "shoulder surfing".

7.7.5 Account passwords should not be revealed to users other than yourself, nor written down and placed in areas of view (e.g. on monitors). Unauthorised access to data by a 3rd party due to negligence could lead to disciplinary procedures.

7.7.6 Where appropriate, physical controls should be used to prevent unauthorised access.

7.8 **Localised Data**

7.8.1 The Trust central systems (purchased and those developed through E-Services, CIS, HR and Finance) are the primary mechanisms by which data should be stored and processed. E.g. The SIMS Management Information System should be the only system used to process student records and affiliated data. Where legacy systems exist (e.g. local “databases” created in Microsoft Access or Excel) consultation needs to be sought with E-Services and the DPO on the most appropriate way of centralising the processes into core systems.

7.8.2 E-Services and School Business Managers cannot be held responsible for the management and protection of internal local databases that are developed without due consideration of risks or consultation. In accordance with the GDPR, the Trust is bound to inform the Information Commissioners Office of data that we hold and process. More information is available at: https://ico.org.uk/about-the-ico/what-we-do/register-of-data-controllers/

The Midland Academies Trust is the registered Data Controller. The record is available online (https://ico.org.uk/ESDWebPages/Entry/Z2337449) and is required to be renewed on 13th December 2018.

7.8.3 E-Services will regularly scan the network for files and their contents that may be in contradiction of the core principles of the GDPR and not already known to through the Information Asset Register.

7.9 **Transfer of Data**

7.9.1 The transfer of data both in and out of the Trust must be protected from possible data breaches and unauthorised access.

7.9.2 Access to portable storage devices is only granted to specific users and/or devices with the approval of the Group Director E-Services. Where data is stored on a portable device it must be encrypted.

7.9.3 Data that is transferred through email must be password protected and compressed into an appropriate format such as a .zip file. Passwords to access the file must be sent in a separate communication to the original file.

7.9.4 Personal data covered by GDPR regulations must never be transferred to a personal email address. There may be an exception to this rule, where data is encrypted following prior authority of the Group Directors for E-Services.

7.9.5 Data must never be transferred outside of the European Economic Area.

7.9.6 Data extracts must be requested to and provided by E-Services to ensure that appropriate data protection legislation and subject consent is applied where appropriate.

7.10 **Software Control**

7.10.1 All software must be purchased through E-Services and no software (including evaluation software) should be installed without permission from E-Services.

7.10.2 A register of Trust owned software will be maintained by E-Services.

7.10.3 Software must not be copied or distributed, as this is an infringement of copyright and therefore illegal - unless specifically permitted by the licensing agreement. This includes attempting to install software from one set of media onto several PCs.

7.10.4 Users are not permitted to use the Trust network to download or store illegal copies of software nor use “keygens”, “serial-sniffers”, “crackz” or other such tools to facilitate the distribution of illegal copies. **This is a serious disciplinary breach.**

7.10.5 All System Software media will be stored securely with E-Services. These are the only proof of a legal license to use the software, and may be required to be produced in evidence should the Federation against Software Theft (FAST) investigate.

7.11 **Quality Assurance and Review**

7.11.1 All staff are expected to ensure that users of the network abide by the policy. Any breach of this policy should be reported in the first instance to a member of the E-Services team who will then define a method for resolution.

7.11.2 This Policy will be reviewed every three years and updated, as applicable, to ensure that it remains appropriate in the light of any relevant changes to the law, organisational policies or contractual obligations