Ormiston Academies Trust

Ormiston Shelfield Community Academy

E-Security Policy

Policy version control

Policy type	Statutory
Author	James Miller OAT DPO
Approved by	OAT Exec, July 2018 Shelfield SLT - D. Lloyd-Jones
Release date	July 2018
Next release date	July 2019
Description of Shelfield changes to OAT model	7.2 Passwords must be changed every 12 months

E-Security Policy

1. Introduction

1.1. At Ormiston Academies Trust (referred to as "The Trust" and any or all of its Academies), we understand that computer technology is an essential resource for supporting teaching and learning. The internet, and other digital and information technologies, open opportunities for pupils and perform an important role in their everyday lives.

Whilst the Trust recognises the importance of promoting the use of computer technology throughout the curriculum, we also understand the need for safe internet access and appropriate use.

The Trust has created this policy with the aim of ensuring appropriate and safe use of the internet and other digital technology devices by all pupils and staff.

The Trust is committed to providing a safe learning and teaching environment for all pupils and staff and has implemented controls to reduce any harmful risks.

The senior ICT technical lead (referred to as "Network Manager"), is a member of staff either appointed by the academy to execute this role or is an existing member of staff within the academy who has additional responsibilities.

This policy will be updated as necessary to reflect best practice, or amendments made to legislation, and shall be reviewed every 12 months from July 2018.

2. Physical Security – Location Access

2.1. All on site devices which store data MUST be kept in a secure location with appropriate access control for example a server room or hub room. Physical access to the server room must be limited to only those individuals who have legitimate responsibilities to justify such access. If the space is left unattended for ANY period, it MUST be secured before leaving. If keys are used, then the keys MUST not be suited to a master key and MUST be clearly marked "Do Not Duplicate"

2.2. Keys allocations must be logged including the date provided. Any losses must also be logged with the appropriate person and key allocations must be fully audited annually.

2.3. Procedures must be in place to ensure access is removed when no longer required. Procedures must also be in place to address lost or stolen keys or access cards. All access to these locations must be audited and must include Names, Time, Date and Reason for access. This log must be kept for a minimum of the last 365 days.

2.4. The academy must ensure compliant arrangements are in place for the removal or relocation of any ICT equipment from its normal location. If temporary storage is required for equipment that contains ANY academy data, then the chosen physical location must also meet the security requirements set out above. Note: these requirements relate to data storage only; you must also consider other policies such as health and safety.

3. Data Processing Equipment locations.

3.1. When considering screen locations for data processors the academy MUST consider the ability to be "over seen". If there is any possibility of the data processors screen been "over seen" this issue must be addressed before the device is used to process ANY academy data.

3.2. Users MUST observe the following precautions when using a device to process or that has access to any academy data:

3.3. Devices are positioned in such a way that information being processed cannot be viewed by person(s) not authorised to view the information. Specific consideration should be given to the siting of devices on which hi risk information is processed or retrieved and high traffic areas such as reception and other public spaces.

3.4. Devices MUST NOT be left logged on when unattended for ANY period of time.

3.5. Accounts MUST NOT be shared with ANY other user for any reason.

3.6. Passwords MUST not be shared with any user, including technical staff. Note: Users may be asked to log into a device for technical staff to carry out maintenance or the technical staff may be required to change your password to carry out required work.

3.7. Users MUST NOT leave hard copies or unencrypted of "Personal Identifiable" digital data unattended at any time, including on the academy grounds unless stored in a secure location that meets the physical security statements set out above. NOTE: Unattended data or data access is considered as a Data Breach and MUST BE reported to your local Data Protection Lead (DPL) for investigation by the Data Protection Officer (DPO).

- For the sake of clarity, the statements above must be adhered to when accessing Academy Data from any device or at any location such as home, public space, friends and family homes, etc. Access to data MUST be secured from other unauthorised users at all times.

4. Inventory

4.1. A requirement of the Trusts building Insurance provider and to meet the obligations of the Data Protection Act 2018 increases the need for securing ICT equipment and as part of the approach OAT is taking, each academy must maintain and keep up to date an audit of ICT equipment.

5. Data Backup

5.1. All data must be backed up to a secure and GDPR Compliant offsite location. Any data that is taken off site or stored offsite for the purpose of backup must be encrypted to a minimum of 256bit. At no point should all data including all backup media exist is a single location. Note: "Offsite" is defined as a location that is not geographically located to or have the same environmental concerns as the main academy site.

5.2. Data stored as backup MUST comply with the academy's policy on data retention. When data reaches "end of life" all data, INCLUDING that stored in ANY backup file in ANY location, MUST also be purged.

5.3. A backup regime MUST allow for any individual piece of data to be recovered in a timely manner. It is accepted that some degree of data loss may occur, but this must not excide more than data produced over the last 24 hours.

5.4. The academy MUST conduct backup testing as set out bellow (or better):

- Daily – Confirm that the last backup has completed successfully. Rectify any issues as necessary.
- Half term – Data integrity check. This can be done by recovering a predefined number of files successfully. This will not require an official test if it has been carried out successfully for a real requirement.
- Termly – Disaster Recovery Total loss test

5.5. Users may backup there data individually, but this backup must meet the required data security principals in this document.

5.6. The Primary Backups should be carried out automatically at set intervals and information contained within these Backups should only be accessible by the ICT Technical Team for verification and restoration. Other backup methods can be used to allow users direct self-recovery of files in addition to a "Primary Backup" but all Backups must meet the storage and security requirements set out in this document.

5.7. The production environment must not be impacted by the running of back-up jobs. All back-ups must be created, scheduled and run according to the performance and availability requirements of the environment.

6. Malware and Virus Detection and Removal

6.1. Malware (malicious software) and Viruses can infiltrate your systems and software and cause damage or allow your systems to be used for malicious or unlawful activities.

6.2. All academy devices MUST Use Anti-virus / Anti-malware detection and removal software at all times. This software MUST be set to scan on access for all devices and updates as a minimum of monthly. Where possible the software must be configured in such a way to stop unauthorised users from disabling it.

6.3. Users MUST NOT disable, and Anti-virus/Anti-Malware software installed on their machine for any reason. If the user has an issue that they believe requires this to happen then they MUST contact a member of the technical team for support.

6.4. Mobile Devices (including academy and personal laptops and mobile phones)

6.5. These devices MUST be encrypted and must be password protected. Encryption level must be equal to or exceed 128bit and the password MUST meet the Password Policy as stated above for laptops. Mobile devices can be secured in several ways but as a minimum MUST have a 4 Digit Pin or better.

6.6. **Please note:** that device accounts are for an individual's use and must not be shared. In another user requires access to the device this MUST be done using an appropriate account for the users and ensure that the user cannot access any data that they are not officially authorised to access.

6.7. All works devices MUST be encrypted, and password protected. When using mobile phones users must be aware of their surroundings and the ability to be "overheard" when discussing personal identifiable information.

6.8. Any device that is used to access or store academy data including contact information or emails MUST be password and / or 4 Digit PIN protected as a minimum.

6.9. If this device is shared with other people outside of the OAT staff, then the device MUST be set in such a way that the data is not accessible by the other users. As this data is classed as offsite this data MUST be encrypted.

6.10. Mobile Phones and Tablets MUST be kept up to date with Apps and Operating Systems. It is the academies responsibility to ensure this is carried out for all academy owned devices. Users MUST ensure that their device meets this requirement.

7. Protecting data with passwords

7.1. All accounts MUST be password protected with complexity set to a minimum of:

- 8 or more characters
- Minimum 1 number
- Minimum 1 uppercase

7.2. Passwords must be changed every 12 months or immediately if you suspect someone has obtained your password or you believe it may have been compromised.

7.3. Passwords MUST NOT be shared with other users unless the account in questions is a Group Access account

7.4. All academies MUST carry out an Annual password audit. This audit MUST include:

- Domain Admin Account including Passwords
- Domain User Account and the full name of the person it is allocated too.
- Other Domain admin account, what they are used for, who has the account details, password
- All hardware accounts (E.g. switches, firewall, etc.) full details and password
- All external accounts (E.g. Office 365 tenancy, Google-Suite, etc.) Account details, password

Please note: No none technical member of staff is permitted to know any Technical management accounts unless signed off by the Principal, this account access must be detailed I the audit including the reason for the access.

Please Note: Audit data MUST be stored in a secure manner with limited access and in a way that allows access to be traced.

8. Patch and Software Updates

8.1. Academies MUST keep all device software and hardware up to date. **Please note:** Software updates MUST be managed and installed at a site appropriate time, agreed beforehand. For general updates it is recommended that these takes place during a significant holiday period to ensure proper testing can take place prior to deployment and to minimise disruption to the academy. ALL critical updates and patches that are issued by hardware and software vendors MUST be implemented as a matter of urgency.

8.2. It is recommended that academies implement Microsoft Windows Server Update Services (WSUS)

8.3. **Please Note:** Other software manufacturers have central deployment methods to roll out software, updates and patches. Always check what functionality is available for your products.