Ormiston Academies Trust

Ormiston Sandwell Community Academy e-Safety & e-Security policy

Policy version control

Policy type	Statutory
Author In consultation with	Les Leese James Miller
Approved by	James Miller, July 2020
Release date	August 2020
Next release date	August 2021
Description of changes	Policy version 1.1: ▪ Dates updated ▪ Minor wording amendments to improve flow and understanding

Contents

1.Introduction

Ormiston Academies Trust (referred to as “the Trust” and any or all of its Academies), understands that computer technology is an essential resource for supporting teaching and learning. The internet, and other digital and information technologies, open up opportunities for pupils and play 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.

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.

“Users” – Any person including staff, students or external

“Network Manager” – Senior ICT Technical Lead person

“Staff” – Any person directly employed by the academy

“Pupil” – Any pupil currently registered to the academy

2.Considerations when using the internet

When accessing the internet, individuals are especially vulnerable to several risks which may be physically and emotionally harmful, including:

2.1. Access to illegal, harmful or inappropriate images

2.2. Cyber bullying

2.3. Access to, or loss of, personal information

2.4. Access to unsuitable online videos or games

2.5. Inappropriate communication with others

2.6. Illegal downloading of files

2.7. Exposure to explicit or harmful content, e.g. involving radicalisation

2.8. Plagiarism and copyright infringement

2.9. Sharing the personal information of others without the individual’s consent or knowledge

3.Roles and responsibilities

3.1. It is the responsibility of all users to ensure that the internet, is used in an appropriate and legal manner. If any users are witnesses to or believe that ANY illegal or harmful activities have taken, or are taking place, they MUST inform an appropriate member of staff immediately.

3.2. The network manager is responsible for the implementation and day to day management of the safety systems and software used within the academy and managing any issues that may arise. This includes ensuring that appropriate filtering is in place for all users and that this is up to date.

3.3. The network manager will provide technical support and advice to members of staff as required and will support any wider academy CPD.

3.4. The Principal will ensure there is a system in place which monitors and supports the network manager, whose role is to work with the Designated Safeguarding Lead (DSL) to carry out the monitoring of e-safety in the academy, keeping in mind data protection requirements.

3.5. The network manager will maintain a log of submitted e-safety reports, incidents and technical issues. All incidents and issues will be reported to the Designated Safeguarding Lead (DSL) and the academy Data Protection Lead (DPL) as appropriate.

3.6. The Academy will ensure that all members of staff are aware of the procedure when reporting e-safety incidents.

3.7. The network manager and DSL will carry out regular reviews of internet usage data by all users and address any concerns as they arise. Proactive monitoring MUST take place and the appropriate staff member MUST be alerted directly and automatically of any incidents.

3.8. Cyber bullying incidents will be reported in accordance with the academy's Anti-Bullying Policy.

3.9. Teachers are responsible for ensuring that e-safety is embedded in the curriculum and safe internet access is always promoted.

3.10. All staff and pupils will ensure they understand and adhere to The Trust's Acceptable Use Policy, which they must sign and return to the Academy. The Academy MUST keep a log of acceptance and this must be updated as changes occur.

3.11. All pupils MUST be made aware of their responsibilities regarding the use of Trust-based ICT systems and equipment, including their expected behaviour.

3.12. All academies MUST meet the minimum requirements of the GDPR ICT Audit or better. If you are unsure or believe that the academy no longer meets this requirement you must inform the DPO immediately.

4.eSafety education

4.1. Educating pupils:

4.1.1. The Academy will regularly update pupils to make sure they are aware of the safe use of new technology both inside and outside of the academy.

4.1.2. Pupils will be taught about the importance of e-safety and are encouraged to be critically aware of the content they access online, including extremist material and the validity of website content.

4.1.3. Pupils will be taught to acknowledge information they access online, to avoid copyright infringement and/or plagiarism.

4.1.4. Clear guidance on the rules of internet use will be present in all classrooms where ICT is used.

4.1.5. Pupils are instructed to report any suspicious use of the internet and digital devices to a member of staff.

4.1.6. The academy will hold e-safety events, such as Safer Internet Day and Anti Bullying Week, to promote online safety.

4.2. Educating staff:

4.2.1. E-safety training opportunities MUST be available to all staff members, including whole academy activities and CPD accredited training courses where appropriate.

4.2.2. All staff will undergo e-safety training including cyber security on an annual basis to ensure they are aware of current issues and any changes to the provision of e-safety, as well as current developments in social media and the internet.

4.2.3. All staff will undergo an annual “Skills Audit” by the academy that will identify individual CPD needs of staff.

4.2.4. All staff will employ methods of good practice and act as role models for pupils when using the internet and other digital devices.

4.2.5. All staff are reminded of the importance of acknowledging information they access online, in order to avoid copyright infringement and/or plagiarism.

4.2.6. Any new staff are required to undergo online safety and awareness training as part of their induction programme, ensuring they fully understand this policy.

4.2.7. The network manager will act as the first point of contact for staff requiring general e-safety advice. Safeguarding issues or concerns MUST be processed using the academies Safeguarding processes.

5.Control Measures

5.1. Internet Access

5.1.1. Internet access will be authorised once parents and pupils have returned the signed consent form in line with The Trust's Acceptable Use Policy.

5.1.2. A record will be kept by the academy of all pupils who have been granted internet access.

5.1.3. All users in Key Stage 2 and above will be provided with usernames and passwords and must keep these confidential to avoid any other pupils using their login details.

5.1.4. Management systems may be in place to allow teachers and members of staff to control workstations and monitor pupils' activity.

5.1.5. Keeping Children Safe in Education compliant filtering systems MUST be in place and in use to reduce any potential risks to pupils through access to, or trying to access, certain websites which are harmful or use inappropriate material.

5.1.6. Any requests by staff for websites to be added or removed from the filtering list must be authorised by the Principal and logged.

5.1.7. All Academy systems MUST be protected by up-to-date anti-virus software.

5.1.8. An agreed procedure will be in place for the provision of temporary users, e.g. volunteers.

5.1.8.1. These accounts MUST be assigned to a single user and logged to ensure that in the event of any abusive, illegal, or behavioral matter can be investigated and allow the investigating office to identify a single individual.

5.1.9. If authorised by the principal, staff can use the internet for lawful and appropriate personal use during out-of-academy hours, as well as break and lunch times. Please Note: All internet activity on academy devices will leave a digital footprint. Any person choosing to use academy devices for personal reasons is giving permission for OAT to have this data until such time that the digital footprint is purged.

5.1.10. Personal use will only be monitored by the network manager, HR or safeguarding staff for access to any inappropriate or explicit sites, where it is justifiable to be necessary and in doing so, and would outweigh the need for privacy.

5.1.11. Inappropriate internet access by a member of staff may result in the staff member being restricted.

6.Social Networking

6.1. Please note: Additional detail is provided in the Staff AUP

6.2. Use of social media on behalf of the academy will be conducted following the processes outlined in The Trust's Social Media Policy.

6.3. Access to social networking sites will be filtered as appropriate.

6.4. Should access be needed to social networking sites for any reason, this will always be monitored and controlled by staff and must be first authorised by the Principal.

6.5. Staff are not permitted to publish comments about the Trust which may affect its reputability.

7. Published content on the academy website and images:

7.1. The Principal will be responsible for the overall content of their academy website and will ensure the content is appropriate and accurate.

7.2. Contact details on the academy website will include the phone number, email and address of the academy.

7.3. Images and full names of pupils, or any content that may easily identify a pupil, must follow the Trust policies relating to the Data Protection Act 2018.

7.4. Pupils are not permitted to take or publish photos of others without permission from the individual and the Academy.

7.5. Staff can take pictures, though they must do so in accordance with academy policies in terms of their sharing and distribution.

7.6. Staff will not take pictures using their personal equipment.

7.7. Any member of staff that is representing the Trust online, e.g. through blogging, must express neutral opinions and not disclose any confidential information regarding the Trust, or any information that may affect its reputability.

8.Mobile devices and hand-held computers:

8.1. The Principal may authorise the use of mobile devices for a pupil and staff where it is seen to be for safety, precautionary or educational use.

8.2. If permitted by the Principal, pupils and staff will access the academy's Bring You Own Device (BYOD) Wi-Fi system using their personal mobile devices and hand-held computers providing the user and/or device meets the academies individual criteria. Internet access will be monitored for any inappropriate use by the network manager when using these devices on the academy network.

8.3. Staff are permitted to use hand-held computers which have been provided by the academy, though internet access will be monitored for any inappropriate use by the network manager and/or DSL.

8.4. Using the academy's devices or network to send inappropriate messages or images is prohibited.

8.5. Personal mobile devices will not be used to take images or videos of pupils or staff.

9.Cyber bullying

9.1. This section must be reviewed alongside the Trust's "Anti-Bullying Policy"

9.2. For the purpose of this policy, cyber bullying is a form of bullying whereby an individual is the victim of harmful or offensive posting of information, images online or direct or indirect messaging.

9.3. The Trust recognises that both staff and pupils may experience cyber bullying and will commit to preventing any instances that occur.

9.4. The academy will regularly educate staff, pupils and parents on the importance of staying safe online, as well as being considerate to what they post.

9.5. The academy will commit to creating a learning and teaching environment which is free from harassment and bullying, for all staff and pupils.

9.6. The Principal will decide whether it is appropriate to notify the police or other appropriate parties regarding any action taken against a pupil or staff member.

10. Reporting misuse

10.1. The Trust will clearly define what is classed as inappropriate behaviour in the Acceptable Use Policy, ensuring all pupils and staff members are aware of what behaviour is expected of them.

10.2. Inappropriate activities are discussed and the reasoning behind prohibiting activities due to e-safety are explained to pupils as part of the curriculum in order to promote responsible internet use.

Misuse by pupils:

10.3. Any instances of misuse should be immediately reported to a member of staff, who will then report this to the Principal.

10.4. Any pupil who does not adhere to the rules outlined in our Acceptable Use Policy and is found to be wilfully misusing the internet, may have their internet access restricted or suspended and a letter sent to their parents explaining the reason for this action.

10.5. Members of staff may decide to issue other forms of disciplinary action to a pupil upon the misuse of the internet. This will be discussed with the Principal and will be issued once the pupil is on the academy premises.

10.6. Complaints of a child protection nature, such as when a pupil is found to be accessing extremist material, shall be dealt with in accordance with the "Child Protection and Safeguarding Policy" and reported to the Designated Safeguarding Lead (DSL).

Misuse by staff:

10.7. Any misuse of the internet by a member of staff should be immediately reported to the Principal.

10.8. The Principal will deal with such incidents in accordance with the “Allegations of Abuse Against Staff Policy” and may decide to take disciplinary action against the member of staff.

10.9. The Principal will decide whether it is appropriate to notify the police of any action taken against a member of staff.

Use of illegal material:

10.10. In the event that illegal material is found on any of the Trust’s networks, or evidence suggests that illegal material has been accessed, the academy must notify the Trust’s Head Office for further investigation and support. Where appropriate the police will be contacted.

10.11. If a child protection incident is suspected, the Trust’s child protection procedure will be followed – the DSL and Principal will be informed, and the police contacted.

11. Physical Security – Location Access

11.1. 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”

11.2. Key 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.

11.3. 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

11.4. 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.

12. Data Processing Equipment locations.

12.1. 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.

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

12.2.1. 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 location of devices on which high risk information is processed or retrieved and high traffic areas such as reception and other public spaces.

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

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

12.2.4. 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.

12.2.5. Users MUST NOT leave unencrypted or hard copies of “Personal Identifiable” 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).

12.2.5.1. 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.

13. Inventory

13.1. 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.

14. Data Backup

14.1. 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 back-up must be encrypted to a minimum of 256bit. At no point should all data including all back-up media exist in 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.

14.2. Data stored as back-up MUST comply with OAT data retention policy. When data reaches "end of life" all data INCLUDING that stored in ANY backup file in ANY location MUST also be purged.

14.3. A back-up 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 exceed data produced over the last 24 hours.

14.4. The academy MUST conduct back-up testing as set out below (or better):

14.4.1. Daily – Confirm that the last back-up has completed successfully. Rectify any issues as necessary.

14.4.2. 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.

14.4.3. Termly – Disaster Recovery Total loss test

14.5. Users may back-up their data individually, but this back-up must meet the required data security principles in this document.

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

14.7. 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.

15. Malware and Virus Detection and Removal

15.1. 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.

15.2. 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.

15.3. Users MUST NOT disable any 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.

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

15.5. 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.

15.6. Please note: that device accounts are for an individual's use and must not be shared. If 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.

15.7. 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.

15.8. 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.

15.9. 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.

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

16. Protecting data with passwords

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

16.1.1. 8 or more characters
16.1.2. Minimum 1 number
16.1.3. Minimum 1 uppercase

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

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

16.4. All academies MUST carry out an annual password audit. This audit MUST include:

16.4.1. Domain Admin Account including Passwords
16.4.2. Domain User Account and the full name of the person it is allocated too.
16.4.3. Other Domain admin account, what they are used for, who has the account details, password
16.4.4. All hardware accounts (E.g. switches, firewall, etc) full details and password

16.4.5. All external accounts (E.g. Office 365 tenancy, Google-Suite, etc) Account details, password

Please note: No non-technical member of staff is permitted to know any technical management accounts unless signed off by the Principal, this account access must be detailed in the audit including the reason for the access.

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

17. Patch and Software Updates

17.1. 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 take 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.

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

17.3. 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.