Ormiston Academies Trust

Ormiston SWB Academy
E-Safety policy

Policy version control

Policy type	Mandatory
Author	Adrian Dellicott
Approved by	James Miller, July 2018
Release date	July 2018
Next release date	July 2019
Description of changes	New policy to comply with GDPR - OAT Role of E-Safety Co-ordinator - ISM Explanation of filtering in place at OSWB Academy - ISM

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. Legal framework

2.1. This policy has due regard to the following legislation, including, but not limited to:

2.1.1. Human Rights Act 1998

2.1.2. General Data Protection Regulation 2018

2.1.3. Freedom of Information Act 2000

2.1.4. Regulation of Investigatory Powers Act 2000

2.1.5. Safeguarding Vulnerable Groups Act 2006

2.1.6. Education and Inspections Act 2006

2.1.7. Computer Misuse Act 1990 amended by the Police and Justice Act 2006

2.1.8. Communications Act 2003

2.1.9. Protection of Children Act 1978

2.1.10. Protection from Harassment Act 1997

2.2. This policy also has regard to the following statutory guidance:

2.2.1. DfE (2016) 'Keeping children safe in education'

2.3. This policy will be used in conjunction with the following trust policies and procedures:

2.3.1. E-security Policy

2.3.2. Anti-Bullying Policy

2.3.3. Social Media Policy

2.3.4. Acceptable Use Agreement

3. Consideration when using the internet

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

3.1.1. Access to illegal, harmful or inappropriate images

3.1.2. Cyber bullying

3.1.3. Access to, or loss of, personal information

3.1.4. Access to unsuitable online videos or games

3.1.5. Loss of personal images

3.1.6. Inappropriate communication with others

3.1.7. Illegal downloading of files

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

3.1.9. Plagiarism and copyright infringement

3.1.10. Sharing the personal information of others without the individual's consent or knowledge

4. Roles and responsibilities

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

4.2. 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.

4.3. The network manager will provide technical support and advice to members of staff as required and will support any wider academy CPD on the Academy's ICT infrastructure.

4.4. The E-safety Co-ordinator will ensure up-to-date with latest developments and issues of concern, publicising these appropriately to staff, students and parents.

4.5. The E-safety Co-ordniator will be in receipt of all e-safety concerns and liaise immediately with the Principal/ Designated Safeguarding Lead (DSL)/ Deputy Designated Safeguarding Leads (DDSL) where concerns are related to child protection/safeguarding.

4.6. 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) and E-Safety Co-ordinator to carry out the monitoring of e-safety in the academy, keeping in mind data protection requirements.

4.7. The Designated Safeguarding Lead (DSL)/Deputy Designated Safeguarding Leads (DDSL) and E-safety Co-ordinator 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)/ Deputy Designated Safeguarding Leads (DDSL) and the academy Data Protection Lead (DPL).

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

4.9. The network manager, DSL and e-safety co-ordinator 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.

4.10. Cyber bullying incidents will be reported in accordance with the academies Anti-Bullying Policy.

4.11. Teachers are responsible for ensuring that e-safety is embedded in the curriculum and safe internet access is promoted at all times.

4.12. 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.

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

5. E-safety education

5.1. Educating pupils:

5.1.1. 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.

5.1.2. 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.

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

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

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

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

5.2. Educating staff:

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

5.2.2. 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 as a whole.

5.2.3. All staff will undergo an annual "Skills Audit" by the academy that will identify individual CPD needs of staff.

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

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

5.2.6. Any new staff are required to undergo online safety and awareness training as part of their induction programme, ensuring they fully understand this E-Safety Policy.

5.2.7. The E-safety Co-ordinator 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.

6. E-safety control measures

6.1. Internet access:

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

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

6.1.3. All users in key stage 3 and above will be provided with usernames and passwords and must keep these confidential to avoid any other pupils using their login details.

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

6.1.5. 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.

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

6.1.7. All Academies systems MUST be protected by up-to-date anti-virus software.

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

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

6.1.9. Staff are able to 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.

6.1.10. 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, would outweigh the need for privacy.

6.1.11. Inappropriate internet access by a member of staff may result in the staff member being restricted. Please see the process outlined in section 8.4 of this policy.

6.1.12. To support the prevention of accessing such extremist, radical or inappropriate materials on the Academy ICT Network we have invested in the use of Smoothwall, which is the Academy firewall and filtering provision. Smoothwall specialises in the education sector, has a two tier checking process as it checks on the Smoothwall network first, and then is checks locally on the Academy ICT network. The Academy use Impero, which is third party software that combines classroom management, network management, and desktop management in one single consolidated solution.

The two technologies do the following:

- Impero software is available within the ICT department class rooms to be used by the teacher within their lessons
- prevent access to unsuitable sites
- prevent unauthorised use of proxy sites
- enforce acceptable usage policy
- create key word libraries for real-time detection
- determine potential risk through key word glossaries with explanations
- create different policies depending on severity
- capture time stamped screen shots of every violation
- add screenshots to log viewer report
- export violations with details and image to PDF
- evidence misconduct from a centralised log to support disciplinary action
- alert the relevant authority when rules are violated
- log and monitor all web activity
- Impero blocks the users instantly for a period of time dependant on the severity of the violation
- Smoothwall blocks users permanently from accessing the internet if required

The monitoring of any breach by students or staff that occurs due to inappropriate online activity via the filtering system is recorded. As a result, an automated report is compiled and emailed to the safeguarding team daily. The report consists of the user activity, which includes:

- username
- date and time stamped
- URL that was accessed
- The reason for it being flagged as a violation

7. Social networking:

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

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

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

7.4. Staff are not permitted to communicate with pupils over personal social networking sites and are reminded to alter their privacy settings accordingly.

7.5. Staff are not permitted to publish comments about the Trust and Academy, which may affect its reputability.

7.6. Staff are not permitted to access social media sites during teaching hours unless it is justified to be beneficial to the material being taught. This MUST be discussed with the Principal prior to accessing the social media site and explicit permission provided.

8. Published content on the academy website and images:

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

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

8.3. 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.

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

8.5. Staff are able to take pictures, though they must do so in accordance with academy policies in terms of the sharing and distribution of such. Staff will not take pictures using their personal equipment.

8.6. 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.

9. Mobile devices and hand-held computers:

9.1. 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

9.2. If permitted pupils and staff will access the academies 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 on the academy premises.

9.3. If permitted pupils and staff are not permitted to access the academy's general use Wi-Fi system at any time using their personal devices.

9.4. Staff are permitted to use hand-held computers that have been provided by the academy, though internet access will be monitored for any inappropriate use by the network manager, DSL and or DDLS when using these on the academy premises.

9.5. Using the academies devices or network to send inappropriate messages or images is prohibited.

9.6. Mobile devices will not be used to take images or videos of pupils or staff.

9.7. The academy will be especially alert to instances of cyber bullying and will treat such instances as a matter of high priority.

10. Network security:

10.1. Please see the Trust's "eSecurity Policy" for additional information

10.2. Each user will be provided with an account name and password. Users will be permitted to change passwords as required and must change them as a minimum every 2 months.

10.3. Passwords have a minimum length of 8 characters including a minimum of 1 number and 1 uppercase character.

10.4. Passwords MUST NOT be shared with other users, if a user becomes aware of another users log on details the user MUST inform a member of staff immediately.

10.5. No "Generic" or "Multi-User" accounts will be created or used by any User unless the accounts are managed in the following way:

10.5.1. The account is assigned to a single individual and the name and time is logged including start and end time.

10.5.2. Once the activity has ended an appropriate member of staff will change the password to something that meets the minimum requirements (this can easily be done by pressing several random keys in the Notepad (or similar) program then copy and paste this into the password field but do NOT save the document)

10.5.3. The change of password is also logged entering user and time of change.

11. Cyber bullying

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

11.2. 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 or images online.

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

11.4. 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 online.

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

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

12. Reporting misuse

12.1. 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.

12.2. 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.

12.3. Misuse by pupils:

12.3.1. Any instances of misuse should be immediately reported to a member of staff, who will then report this to the DDSL/DDSL and e-safety co-ordindator using the report process.

12.3.2. Any pupil who does not adhere to the rules outlined in our Acceptable Use Policy and is found to be wilfully misusing the internet, will have a letter sent to their parents explaining the reason for suspending their internet use.

12.3.3. 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.

12.3.4. 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) or Deputy Designated Safeguarding Lead (DDDL).

12.4. Misuse by staff:

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

12.4.2. 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.

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

12.5. Use of illegal material:

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

12.5.2. Incidents will be immediately reported to the "Internet Watch Foundation" and the police will be contacted if the illegal material is, or is suspected to be, a child sexual abuse image hosted anywhere in the world, a non-photographic child sexual abuse image hosted in the UK, or criminally obscene adult content hosted in the UK.

12.5.3. 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.