# Ormiston Shelfield Community Academy

# E-Safety Policy

Date adopted: September 2018 Next review date: July 2019

**Policy Version Control**

| | |
|---|---|
| Policy prepared by | OAT Manditory Policy |
| Responsible committee | SLT - D. Lloyd-Jones – Assistant Principal |
| Date approved by committee | September 2018 |
| Date ratified by LGB (if required) | n/a |
| Description of changes from the model policy | - |

Achieving more together

# Statement of intent

At Ormiston Shelfield Community Academy, we understand that computer technology is an essential resource for supporting teaching and learning. The internet, and other digital and information technologies, open up opportunities for students and play an important role in their everyday lives.

Whilst the academy 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.

Our academy has created this policy with the aim of ensuring appropriate and safe use of the internet and other digital technology devices by all students and staff.

The academy is committed to providing a safe learning and teaching environment for all students and staff, and has implemented important controls to prevent any harmful risks.

To be read alongside:
The Acceptable User Agreement
Social Media Policy
Safeguarding Policy
Anti-Bullying Policy
Prevent Policy

# Use of the Internet

The academy understands that using the internet is important when raising educational standards, promoting student achievement and enhancing teaching and learning. (KCSIE 2018)

Internet use is embedded in the statutory curriculum and is therefore an entitlement for all students, though there are a number of controls the academy is required to implement to minimise harmful risks.

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

- Access to illegal, harmful or inappropriate images
- Cyber bullying
- Access to, or loss of, personal information
- Access to unsuitable online videos or games
- Loss of personal images
- Inappropriate communication with others
- Illegal downloading of files
- Exposure to explicit or harmful content, e.g. involving radicalisation
- Plagiarism and copyright infringement
- Sharing the personal information of others without the individual's consent or knowledge

Ormiston Academies Trust

Achieving more together

# Roles and Responsibilities

It is the responsibility of all staff to be alert to possible harm to students or staff due to inappropriate internet access or use, both inside and outside of the academy, and to deal with incidents of such as a priority.

The governing body is responsible for ensuring that there are appropriate filtering and monitoring systems in place to safeguard students. This will be achieved via the LGB and OATs ICT Compliance Audit.

The E-safety Officer, (Mr Lloyd-Jones), is responsible for ensuring the day-to-day e-safety in the academy, and managing any issues that may arise.

The Principal is responsible for ensuring that the E-safety Officer and any other relevant staff receive CPD to allow them to fulfil their role and train other members of staff.

The E-safety Officer will provide relevant training and advice for members of staff as part of the requirement for staff to undergo regularly updated safeguarding training and be able to teach students about online safety.

The Principal will ensure there is a system in place which monitors and supports the E-safety Officer, whose role is to carry out the monitoring of e-safety in the academy, keeping in mind data protection requirements.

The E-safety Officer will regularly monitor the provision of e-safety in the academy and will provide feedback to the Principal.

E-safety incidents are logged through our filtering systems and distributed to the appropriate member of the Pastoral Team. E-safety incidents are investigated and recorded on Sims as a behaviour management concern. Serious concerns are escalated to the DSL.

The academy has an established procedure for reporting incidents and inappropriate student internet use, either by students or staff. Members of the Children's Services Team receive a report each day from the academy Smoothwall filtering system with searches that are flagged as inappropriate. These are checked for legitimacy and followed up if necessary with appropriate disciplinary action.

A report that containes flagged searches or possible innaprorpate content from staff accounts is sent to the E-safety Officer each day. These are checked for legitimacy and if necessary, its details would be passed onto the Principal where the staff disciplinary procedure would be followed, as appropriate.

The E-safety Officer will ensure that all relevant members of staff are aware of the procedure when reporting e-safety incidents, and will keep a log of all incidents recorded.

Staff are aware of the Social Media Policy which gives clear guidelines regarding staff conduct when using social media. Personal social media is blocked on site for both staff and students.

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

The governing body will hold regular meetings with the E-safety Officer to discuss the effectiveness of the e-safety provision, current issues, and to review incident logs, as part of the academy's duty of care.

Ormiston Academies Trust will review the policy annually and delegate to the governing body to evaluate the implementation of the policy.

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

All staff are responsible for ensuring they are up-to-date with current e-safety issues, and this E-Safety Policy.

All staff and students will ensure they understand and adhere to our Acceptable Use Agreement, which is agreed to electronically and stored centrally.

Parents are responsible for ensuring their child understands how to use computer technology and other digital devices appropriately. The academy will support parents by sharing information and links through a dedicated section of the academy website.

The academy uses a designated section of the academy website to update stake holders on e-safety. These are also periodically distributed through our social media channels. The e-safety area of the website and its content are also brought to the attaention of our academy Parent Forum for their attention and input.

All students are aware of their responsibilities regarding the use of academy-based ICT systems and equipment, including their expected behaviour.

# E-safety Education

### Educating students:

- An e-safety programme will be established and delivered to students in an age-appropriate manner so that all develop an awareness of how to use the internet safely both inside and outside of the academy.
- Students 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.
- Students will be taught to acknowledge information they access online, in order to avoid copyright infringement and/or plagiarism.
- Clear guidance on the rules of internet use will be presented in all students at the log in screen.
- Students will be made aware as to how to report any inappropriate use of the internet and digital devices, and be told that it is their responsibility to do so. The academy will establish and publicise a mechanism by which students can anonymise reports should they find this necessary.'
- The taught curriculum will be used to educate students about cyber bullying, including how to report cyber bullying, the social effects of spending too much time online and where to access help.
- The academy will hold such e-safety events as are necessary and appropriate in order to promote online safety effectively, such as Safer Internet Day and Anti Bullying Week,

### Educating staff:

- A planned calendar programme of e-safety training opportunities is available to all staff members, including whole academy activities and CPD training courses.
- All staff will undergo e-safety training annually or when changes occur basis to ensure they are aware of current e-safety issues and any changes to the provision of e-safety, as well as current developments in social media and the internet as a whole.
- All staff will employ methods of good practice and act as role models for students when using the internet and other digital devices.
- All staff will be educated on which sites are deemed appropriate and inappropriate.
- All staff are reminded of the importance of acknowledging information they access online, in order to avoid copyright infringement and/or plagiarism.
- Any new staff are required to undergo e-safety training as part of their induction programme, ensuring they fully understand this E-Safety Policy/Social Media Policy/User Agreement.
- The e-safety officer will act as the first point of contact for staff requiring e-safety advice.

### Educating parents:

- E-safety information will be directly delivered to parents through a variety of formats, the academy website and social media.
- Parents' Evenings, meetings and other similar occasions will be utilised to inform parents of any e-safety related concerns.

## E-safety Control Measures

### Internet access:

- Parents are given the Acceptable Use Policy alongside data capture forms on New Intake Evening.
- All students must agree to the Acceptable Use summary before they log into a computer.
- All users will be provided with usernames and passwords, and are advised to keep these confidential to avoid any other students using their login details.
- Management systems will be in place to allow teachers and members of staff to control workstations and monitor Students" activity.
- Effective filtering systems will be established to eradicate any potential risks to students through access to, or trying to access, certain websites which are harmful or use inappropriate material.
- The governing body will ensure that use of appropriate filters and monitoring systems does not lead to 'over blocking', such that there are unreasonable restrictions as to what students can be taught with regards to online teaching and safeguarding.
- Any requests by staff for websites to be added or removed from the filtering list must be first authorised by the E-safety Officer
- All academy systems will be protected by up-to-date anti-virus software.
- An agreed procedure will be in place for the provision of temporary users, e.g. volunteers.
- Staff are able to use the internet for personal use during out-of-academy hours, as well as break and lunch times.
- Personal use will only be monitored by the E-safety Officer 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.
- Inappropriate internet access by staff may result in the staff member being permitted to use the internet for academy purposes only, and prohibited from using any personal devices. This will be dealt with following the process outlined in the staff disciplinary policy.

### Email:

- No sensitive personal data shall be sent to any other students, staff or third parties via works email.
- Students are made aware that all email messages are monitored and that the filtering system will detect inappropriate links, viruses, malware and profanity.
- Staff members are aware that their email messages maybe monitored.
- Any emails sent by students (either internal or external) will be subject to the same guidelines and expectations as set out in the Acceptable Use Policy.
- The academy uses Microsoft Office 365 filtering systems to detect, deny/quarantine chain letters, spam and emails from unknown sources that are suspected to be malicious.

Achieving more together

# Social Networking

- Use of social media on behalf of the academy will be conducted following the processes outlined in our Staff Code of Conduct.
- Access to social networking sites is blocked. Requests for sites that are for education resources can be requested.
- 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 Mr Lloyd-Jones (Assistant Principal).
- Students are regularly educated on the implications of posting personal data online outside of the academy.
- Staff are regularly educated on posting inappropriate photos or information online, which may potentially affect their position and the academy as a whole.
- Staff are not permitted to communicate with students over social networking sites and are reminded to alter their privacy settings.
- Staff are not permitted to publish comments about the academy which may reasonably be expected to occasion reputational damage.
- 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 will be discussed with the Principal prior to accessing the social media site.

# Published Content on the Academy Website

- Mr Lloyd-Jones will be responsible for the overall content of the website, and will ensure the content is appropriate and accurate.
- Contact details on the academy website will include the phone number, email and address of the academy – no personal details of staff or students will be published.
- Images and full names of students, or any content that may easily identify a student, will be selected carefully, and will not be posted until authorisation from parents has been received.
- Students are not permitted to take or publish photos of others without permission from the individual.
- 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.
- Any member of staff that is representing the academy online, e.g. through blogging, must express neutral opinions and not disclose any confidential information regarding the academy, or any information that might cause reputational damage to the academy or any persons associated with it.

# Mobile Devices and Hand-held Computers

- Mobile devices are permitted to be used by students before academy, breaktime and lunchtime.
- 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 E-safety Officer when using these on the academy premises.
- The sending of inappropriate messages or images from mobile devices is prohibited.
- The academy will be especially alert to instances of cyber bullying and will treat such instances as a matter of high priority.

# Network Security

- Network profiles for each student and staff member are created, in which the individual must enter a username and personal password when accessing the ICT systems within the academy.
- Passwords have a minimum and maximum length, to prevent 'easy' passwords or mistakes when creating passwords.
- Passwords will expire after 365 days

# Cyber Bullying

- 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.
- The academy recognises that both staff and students may experience cyber bullying and will commit to preventing any instances that should occur.
- The academy will regularly educate staff, students and parents on the importance of staying safe online, as well as being considerate to what they post online.
- Students will be educated about online safety through teaching and learning opportunities as part of a broad and balanced curriculum; this includes covering relevant issues within PSHE lessons as well as sex and relationship education.
- The academy will commit to creating a learning and teaching environment which is free from harassment and bullying, ensuring the happiness of all members of staff and students.
- The academy has zero tolerance for cyber bullying, and any incidents will be treated with the upmost seriousness and will be dealt with in accordance with our Anti-Bullying Policy.
- The Principal will decide whether it is appropriate to notify the police or anti-social behaviour coordinator within their LA of the action taken against a student.

# Reporting Misuse

- Ormiston Shelfield Community Academy will clearly define what is classed as inappropriate behaviour in the Acceptable Use Agreement, ensuring all students and staff members are aware of what behaviour is expected of them.
- Inappropriate activities are discussed and the reasoning behind prohibiting activities due to e-safety are explained to students as part of the curriculum in order to promote responsible internet use.

### Misuse by students:

- Teachers have the power to discipline students who engage in misbehaviour with regards to internet use.
- Any instances of misuse should be immediately reported to a member of staff, who will then report this to the Principal.
- Students who do not adhere to the AUP will be dealt with according to the academy's Behaviour Policy.
- Members of staff may decide to issue other forms of disciplinary action to a student upon the misuse of the internet. This will be discussed with the Principal.
- Complaints of a child protection nature, such as when a student is found to be accessing extremist material, shall be dealt with in accordance with our Child Protection and Safeguarding Policy.

### Misuse by staff:

- Any misuse of the internet by a member of staff should be immediately reported to the Principal.
- 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.
- The Principal will decide whether it is appropriate to notify the police or anti-social behaviour coordinator in their LA of the action taken against a member of staff.