Cliff Park Ormiston Academy

E-Safety Policy

Date adopted: *30 September 2018* Next review date: *30 September 2019*

Policy Version Control

Policy prepared by	OAT Mandatory Policy
Responsible committee	Local Governing Body

Statement of intent

At Cliff Park Ormiston 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 pupils and play an important role in their everyday lives.

Whilst the school 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 school 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 school is committed to providing a safe learning and teaching environment for all pupils and staff, and has implemented important controls to prevent any harmful risks.

To be read alongside:

The Accaeptable User Agreement
Social Media Policy
Mobile Devices Policy
Safeguarding Policy
Anti-Bullying Policy
Prevent Policy

Use of the Internet

The school understands that using the internet is important when raising educational standards, promoting pupil achievement and enhancing teaching and learning. (KCSIE 2016)

Internet use is embedded in the statutory curriculum and is therefore an entitlement for all pupils, though there are a number of controls the school 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

Roles and Responsibilities

It is the responsibility of all staff to be alert to possible harm to pupils or staff due to inappropriate internet access or use, both inside and outside of the school, 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 pupils. This will be achieved via the LGB and OATs ICT Compliance Audit.

The e-safety officer, Mr J. Jones, is responsible for ensuring the day-to-day e-safety in the school, 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 pupils 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 school, keeping in mind data protection requirements.

The e-safety officer will regularly monitor the provision of e-safety in the school and will provide feedback to the Principal.

The e-safety officer will oversee a log of submitted e-safety reports and incidents.

The e-safety officer will establish a procedure for reporting incidents and inappropriate internet use, either by pupils or staff.

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.

Cyber bullying incidents will be reported in accordance with the school’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 school’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 pupils will ensure they understand and adhere to our Acceptable Use Agreement, which they agree to electronically every time they sign into the school network, and is available on the school website.

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 brochures and website links.

The e-safety officer is responsible for communicating with parents regularly and updating them on current e-safety issues and control measures.

All pupils are aware of their responsibilities regarding the use of school-based ICT systems and equipment, including their expected behaviour. This is re-iterated at the beginning of each academic year by the IT faculty in lessons.

E-safety Education

Educating pupils:

- An e-safety programme will be established and delivered to pupils 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.
- 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.
- Pupils 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 the pupil AUP.
- Pupils 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 pupils can make anonymise reports should they find this necessary.'
- The taught curriculum will be used to educate pupils 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 school activities and CPD training courses.
- All staff will undergo e-safety training on an annual 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 pupils 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, including brochures, the school website and other e-safety websites.
- 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:

- Internet access will be authorised once pupils have signed in and accepted the terms of the Acceptable Use Agreement.
- All users will be provided with usernames and passwords, and are advised to keep these confidential to avoid any other pupils using their login details.
- Pupils' passwords will be changed annually and their activity is continuously monitored by the e-safety officer.
- Management systems will be in place to allow teachers and members of staff to control workstations and monitor pupils' activity.
- Effective filtering systems will be established to eradicate any potential risks to pupils through access to, or trying to access, certain websites which are harmful or use inappropriate material.
- Filtering systems will be used which are relevant to pupils' age ranges, their frequency of use of ICT systems, and the proportionality of costs compared to risks.
- 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 pupils 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/Principal.
- All school 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.
- There is no master list of passwords due to the fact they are encrypted an inaccessible. Procedures will be put in place to allow access to accounts when activity needs to be monitored.
- While staff are able to use the internet for personal use during out-of-school hours, as well as break and lunch times, it is strongly suggested that they do not save passwords on school systems or use school systems for personal accounts, such as using school email for personal Amazon or eBay accounts.
- Personal use will only be monitored by the e-safety officer/Principal 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 will be dealt with following the process outlined in the staff disciplinary policy.

Email:

- The use of personal email accounts to send and receive personal data or information is prohibited.
- No sensitive personal data shall be sent to any pupils, staff or third parties.
- Pupils 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 may be monitored if it is suspected that they have been used innapropriately or a safeguarding issue arises involving them.
- Any emails sent by pupils to external organisations will be overseen by their class teacher and must be authorised before sending.
- Chain letters, spam and all other emails from unknown sources will be deleted without opening. If these are passed on internally, disciplinary procedures will be followed.

Social Networking

- Use of social media on behalf of the school will be conducted following the processes outlined in our Staff Code of Conduct.
- Access to social networking sites will be filtered as appropriate.
- 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.
- Pupils are regularly educated on the implications of posting personal data online outside of the school.
- Staff are regularly educated on posting inappropriate photos or information online, which may potentially affect their position and the school as a whole.
- Staff are not permitted to communicate with pupils over social networking sites and are reminded to alter their privacy settings.
- Staff are not permitted to publish comments about the school 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

- The Principal will be responsible for the overall content of the website, and will ensure the content is appropriate and accurate.
- Contact details on the school website will include the phone number and address of the school – no personal details of staff or pupils will be published. Email contact will be via a website contact form.
- Images and full names of pupils, or any content that may easily identify a pupil, will be selected carefully, and will not be posted until authorisation from parents has been received. This will be done in line with GDPR and no personal information will be published publicly.
- Pupils 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 school policies in terms of the sharing and distribution of such. Staff will not take pictures using their personal equipment.
- Any member of staff that is representing the school online, e.g. through blogging, must express neutral opinions and not disclose any confidential information regarding the school, or any information that might cause reputational damage to the academy or any persons associated with it.

Mobile Devices and Hand-held Computers

- The Principal may authorise the use of mobile devices by a pupil where it is seen to be for safety or precautionary use.
- Pupils are not permitted to access the school's Wi-Fi system at any times using their personal mobile devices and hand-held computers.
- Mobile devices are not permitted to be used during school hours by pupils. Staff may use mobile devices when not teaching or carrying out directed tasks such as duties.
- Staff are permitted to use hand-held computers which have been provided by the school, though internet access will be monitored for any inappropriate use by the e-safety officer when using these on the school premises.
- The sending of inappropriate messages or images from mobile devices is prohibited.
- Mobile devices will not be used to take images or videos of pupils or staff unless instructed by the Principal.
- The school 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 pupil and staff member are created, in which the individual must enter a username and personal password when accessing the ICT systems within the school.
- Passwords have a minimum and maximum length and complexity requirements, to prevent ‘easy’ passwords or mistakes when creating passwords.
- Passwords will expire after 1 year to ensure maximum security for pupil and staff accounts.
- Passwords should be stored using non-reversible encryption.
- Passwords must never be shared with anyone other than the account holder, within school or outside of school, for any reason.

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 school recognises that both staff and pupils may experience cyber bullying and will commit to preventing any instances that should occur.
- The school will regularly educate staff, pupils and parents on the importance of staying safe online, as well as being considerate to what they post online.
- Pupils 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 school 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 pupils.
- The school 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 headteacher will decide whether it is appropriate to notify the police or anti-social behaviour coordinator in their LA of the action taken against a pupil.

Reporting Misuse

- Cliff Park Ormiston Academy will clearly define what is classed as inappropriate behaviour in the Acceptable Use Agreement, ensuring all pupils 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 pupils as part of the curriculum in order to promote responsible internet use.

Misuse by pupils:

- Teachers have the power to discipline pupils 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 e-safety officer or Principal.
- Pupils 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 pupil upon the misuse of the internet. This will be discussed with the Principal.
- 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 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.

Use of illegal material:

- In the event that illegal material is found on the school's network, or evidence suggest that illegal material has been accessed, the police will be contacted.
- 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.
- If a child protection incident is suspected, the school's child protection procedure will be followed – the DSL and Principal will be informed and the police contacted.

The scheduled review date for this policy is: 30 September 2019

OAT Ormiston Academies Trust

Achieving more together

ICT Code of Conduct and Acceptable Use Policy (Staff)

All staff issued with an Academy ICT user account are required to sign the following agreement and adhere to its contents at all times. Any concerns or clarification of the points below, or suspected breaches of this agreement, should be discussed with the Principal.

Use of ICT Equipment:

- I will only use the Academy's ICT equipment, e-mail, Internet and any related technologies for professional purposes, or for uses deemed reasonable.
- I will not install any hardware or software on to academy ICT equipment, or connect any non-academy-owned equipment without permission of the ICT Team.
- I will not move or remove any ICT equipment or peripherals within or to/from the academy without permission of the ICT Team.
- I understand that any personally-owned ICT equipment (laptops, tablets, mobile phones, and other devices) are brought on to the academy site at my own risk, and the supervision and security of any equipment is solely my responsibility. ***The academy will take no responsibility for the loss or theft of any such item.***

Data Security:

- I will comply with ICT system security and password protocols set by the academy ICT Team.
- I will not disclose any passwords provided to me by the academy or other related authorities to any other party.
- I will not allow any student or other staff member to use a computer logged in to my account.
- I will only use the approved, secure email system(s) for academy business.
- I will ensure that personal data (e.g. student/staff data) is kept secure, is used appropriately, and is not made available to other parties, whether in the academy or accessed remotely off site.
- I will only access academy data via local data storage or via the academy's google drive
- I will not remove data or files from academy premises (via a memory stick/other media) without the permission of the ICT Team; where permission is given I will ensure any data removed is encrypted.
- I will not save data or files relating to academy business on personal ICT equipment. I will ensure that all data or files accessed off-site are saved to my academy user area via google.drive
- I will respect copyright and intellectual property rights.

Communication Etiquette:

- I will ensure that all electronic communications with students, staff, parents and external contacts are compatible with my professional role.
- I will respect professional and personal etiquette in all electronic communications.
- I will ensure that any comments about students (such as positive and negative events on SIMS) are factual and non-judgemental, do not mention other students, and contain nothing that I would not be prepared to discuss in person to that student or their parent/carer.
- I will ensure that my online activity, both in and outside the academy, will not bring my professional role into disrepute.
- I will not browse, download, upload or distribute any material that could be considered offensive, illegal or discriminatory. ***Publication of any material relating to the academy, its operations, its staff or its students that could be regarded as derogatory, is a disciplinary offence which could lead to dismissal.***
- I will not post comments relating to the academy, its staff, students or business practices or performance, use its logo, or make comments that appear to be on behalf of the academy, on my own or other's social media accounts.

Safeguarding/Safer Working Practice:

- I will support and promote the academy's Safeguarding Policy and help pupils to be safe and responsible in their use of ICT and related technologies.
- I will not give out my own personal details, such as mobile phone number and personal email address, to students, or friend them/communicate with them on social networking sites.
- I will ensure that images of students and/or staff will only be taken, stored and used for professional purposes in line with academy policy and with the consent of the parent, carer or staff member. I will not distribute images outside the academy network without the permission of the student's parent/carer or member of staff, and the Principal.
- I will support the academy's approach to online safety and not e-mail, upload or add any images, video, sounds or text to any internal or external site that could upset or offend any member of the academy community.

User Declaration:

The text below will be displayed to staff when they login to an academy computer. The response will be data logged by the network. The academy will not require the need to keep paper copies of a signed declaration.

"By pressing OK and signing in to any academy device or using academy IT systems, you agree to abide by the staff or student Acceptable Use Policy available on the Cliff Park website under Policies. Failure to abide by the rules in this policy as it applies to a staff member or student will result in disciplinary action."

I understand that all my use of the Internet and other related technologies can be monitored and logged and can be made available, on request, to the Principal.

I agree to follow this Code of Conduct and to commit to safe and reputable use of ICT equipment in the course of my professional duties in and outside of the Academy. I understand that violation of this agreement will be investigated and may result in disciplinary action, which could involve sanctions up to and including dismissal.

OAT Ormiston Academies Trust

Achieving more together

ICT Code of Conduct and Acceptable Use Policy (Student)

Rationale

The increasing use of ICT in all aspects of life including education, training & employment means that students must train themselves in the responsible use of ICT systems.

Guidelines

1. Academy-provided login accounts - Each student is provided with a unique login name for the network, Google and other software and systems, which is password protected. Whilst logged in the student must take precautions that no other person uses their terminal. Each student is responsible for any access to the network using their login name and so must keep their password secret. Any misuse that occurs under a login will result in disciplinary action being taken against that student.
2. Document Storage - Each student is provided with enough storage via google drive, an online storage solution that can be accessed through a computer, tablet or mobile phone. Personal documents including, but not limited to, images, videos, games, audio files etc should not be stored at the academy. Pen Drives or other mobile storage devices should not be used.
3. Internet - This is provided as an educational tool for student research. Undesirable sites have mostly been blocked. If one is discovered by accident it must be reported to IT Desk (help@cliffparkoa.co.uk) and your ICT Teacher who will block it. Any student who knowingly gains access to an undesirable site or bypasses a block to access a site will face disciplinary action.
4. Computer Games - There may be times when a teacher will authorise the use of games for academic and/or enrichment purposes, but besides these occasions no computer game playing is permitted in the academy. Students found playing computer games will face disciplinary action.
5. E-mail - Student e-mail is provided as an aid to learning. Any student who abuses this facility will face disciplinary action. Make sure that only the intended recipients are present in the To and Cc boxes. If received, abusive e-mails should be reported to a member of staff. Abuse includes:

   - Sending or forwarding e-mails containing libelous, defamatory, offensive, racist or obscene content such as bad language, threats, insults etc. or anything that can be construed as bullying.
   - Sending mass e-mails or forwarding chain letters.
   - Sending games, game links or other inappropriate subject matter.

Disciplinary Action

Any abuse of computer facilities will result in a “Consequence” for the student concerned. It may also result in the student having their network account disabled. Serious breaches of this code of conduct could result in more extensive consequences in line with the academy’s Behaviour Policy, including the possibility of exclusion/Permanent Exclusion from the academy.

User Declaration:

The text below will be displayed to staff when they login to an academy computer. The response will be data logged by the network. The academy will not require the need to keep paper copies of a signed declaration.

“By pressing OK and signing in to any academy device or using academy IT systems, you agree to abide by the staff or student Acceptable Use Policy available on the Cliff Park website under Policies. Failure to abide by the rules in this policy as it applies to a staff member or student will result in disciplinary action.”

I understand that all my use of the Internet and other related technologies can be monitored and logged and can be made available, on request, to the Principal.

I agree to follow this Code of Conduct and to commit to safe and reputable use of ICT equipment in the course of my professional duties in and outside of the Academy. I understand that violation of this agreement will be investigated and may result in disciplinary action, which could involve sanctions up to and including exclusion from the academy.