



# **E-SAFETY POLICY (Academies)**

**The OHC&AT Board of Directors has agreed this Policy and as such, it applies across all OHCAT Academies – 2<sup>nd</sup> July 2021.**

Jay Mercer  
Chair of OHCAT Board

A handwritten signature in black ink, appearing to read "Jay Mercer", is positioned below the printed name and title.

# E-Safety Policy

## INTRODUCTION

Orchard Hill College and Academy Trust (OHC&AT) is a 'family' of providers, comprising Orchard Hill College (OHC) and Orchard Hill College Academy Trust (OHCAT), which works together for mutual benefit. OHC&AT is committed to providing outstanding educational opportunities for all our pupils and students. The safety and welfare of our pupils and students is of the utmost importance. Ensuring that pupils and students can safely access new technology and learn how to participate in the digital world without compromising their safety and security is a key part of delivering a well-rounded programme of education.

This policy sets out how we will keep pupils/students at OHCAT Academies safe, whether using new technology within OHCAT provision or at home, including accessing remote learning. There is a separate policy for Orchard Hill College.

This policy has been written with reference to a range of guidance including Keeping Children Safe in Education (DfE, 2020), 'Teaching online safety in schools' (DfE, 2019), the 'Education for a Connected World' framework (UKCIS, 2020), 'Relationships and sex education (RSE) and health education (DfE, 2020), the London Grid for Learning (LGfL) E-Safety Policy and the South West Grid for Learning (SWGFL) E-Safety Policy. The policy is also informed by government guidance on the Prevent duty and Channel. E-safety represents a crucial strand of safeguarding children and vulnerable adults, and such this policy should be read in conjunction with OHC&AT's Child Protection, Adult Protection and Safeguarding Policy and Procedures, as well as the related policies and procedures listed at the end of the document. Delivering high quality e-safety education also forms part of the universal safeguarding provision detailed in each Academy's Safeguarding & Wellbeing Offer.

This policy applies to all members of the OHC&AT community including staff, pupils/students, apprentices, volunteers, families, visitors, external professionals and community users who have access to OHC&AT's ICT system.

## E-SAFETY IN ACADEMIES

The impact of technology on the lives of all citizens increases yearly, particularly for children and young people who are keen to explore new and developing technologies. Technology is transforming the way that schools teach and children learn. At home, technology is changing the way children live and the activities in which they choose to partake. Developing technology brings opportunities; it also brings risks and dangers. Keeping Children Safe in Education (2020) categorises these as:

- content: being exposed to illegal, inappropriate or harmful material; for example pornography, fake news, racist or radical and extremist views;

- contact: being subjected to harmful online interaction with other users; for example commercial advertising as well as adults posing as children or young adults; and
- conduct: personal online behaviour that increases the likelihood of, or causes, harm; for example making, sending and receiving explicit images, or online bullying.

Within these categories, risks to pupils and students using new technologies may include, but are not limited to:

- Access to illegal, harmful or inappropriate images or other content
- Unauthorised access to, loss of, and sharing of personal information
- Internet grooming
- Extremism and radicalisation
- Child criminal exploitation (CCE) and/or child sexual exploitation (CSE)
- The sharing and distribution of personal images without consent
- Inappropriate communication and contact with others
- Cyber-bullying
- Sexting
- Access to unsuitable video and internet games
- Misinformation and disinformation
- Plagiarism and copyright infringement
- Illegal downloading of music or video files
- Excessive use which may impact on social and emotional development and learning

## **ROLES AND RESPONSIBILITIES**

Each OHCAT Academy has a named E-Safety Lead, who will work with the Designated Safeguarding Lead to oversee and manage the recording, investigation and resolution of cyberbullying and any other incidents which fall within the remit of this policy.

Pupils/students at OHCAT Academies may bring their own mobile and tablet devices to school, including devices that are used as communication aids. Each provision has a clear process in place for managing the use of personal devices during school hours, which is set out in the relevant Child Protection, Adult Protection & Safeguarding Policy. OHCAT does not accept responsibility for any damage to personal devices while at school.

OHCAT Academies also work with OHC's Digital School to support the development and delivery of ICT through student-led digital workshops and initiatives. Pupils/students are supported to use games appropriately and only in designated time slots. The Digital School also works with pupils/students around the dangers of online gaming and meeting people online, as well as risks relating to 'fake news' and other misinformation/disinformation including conspiracy theories, and has developed a number of bespoke resources to support pupils/students with SEND to understand these topics.

All OHCAT staff will familiarise themselves with this policy. E-safety is included in discrete lessons and throughout the year through other vehicles, such as assemblies and themed activities e.g. Anti-Bullying Week. Staff are reminded of their e-safety obligations via regular updates, training and discussion throughout the year.

Each OHCAT Academy has a Governor responsible for Safeguarding and Child Protection, who will monitor adherence to the policy, together with the E-Safety Lead, and feedback to the Local Governing Body as appropriate.

### **OHCAT Academies will monitor the impact of this policy using:**

- Logs of reported incidents (maintained by the E-Safety Lead).
- Monitoring of the Academy's network where necessary.
- Regular monitoring of the Academy's social media presence.
- Monitoring of the Academy's Google Apps platform where necessary.
- Monitoring of all remote learning platforms where necessary, including Zoom and Microsoft Teams.
- Monitoring of the Academy's internet access where necessary, and regular reviews of the Academy's website filtering.
- Parent/carer questionnaires.

### **CREATING A SAFE ICT INFRASTRUCTURE**

All users of OHCAT Academy computer networks have clearly defined access rights, managed via a username and password login system. Account privileges are achieved through the file and folder permissions, and are based upon each user's requirements. Pupil/student accounts are restricted and do not allow access to all network drives. Guests are required to log in using a visitor login that has limited network access.

A permanently-enabled filtering system is used to filter inappropriate material. Additionally web pages are scanned for content as requested. Any changes to setting have to be requested through the OHC&AT IT Helpdesk. All changes made to Internet filtering are logged. Security software is installed on all computers.

Staff should be aware that Internet traffic is monitored and can be traced to the individual user. It is the responsibility of the user to ensure that they have logged off the system when they have completed their task and to keep their user credentials confidential.

Please refer to the OHC&AT IT Acceptable Use Policy for further details.

### **Rules for publishing material online (including images of pupils/students)**

Academy websites are a valuable tool for sharing information and promoting pupils' and students' achievements. We recognise the potential for abuse. Therefore the following principles will always be considered:

- If an image, video or audio recording of a pupil/student is used, their surname should not be used (including in credits).
- Staff **must not** take photographs of pupils or students using their personal devices – all pupil/student photographs must be taken using OHC&AT equipment and transmitted through OHC&AT systems.
- Files should be appropriately named in accordance with these principles.
- Only images of pupils/students in suitable dress should be used and group photographs are preferred (though not exclusively) in preference to individual photographs.
- Parents/carers are given the opportunity to withdraw permission for the Academy to publish images/audio/video of their child on the Academy website.
- Content should not infringe the intellectual property rights of others – copyright may apply to text, images, music or video that originate from other sources. All copied or embedded content should be properly referenced.
- Content should be polite and respectful.
- Material should be checked by a member of the Academy's Senior Leadership Team before being published.
- Staff must not post or transmit images of pupils/students or families via their personal social media accounts. OHC&AT considers social media to be any technology-based platform used for interacting or discussion via voice, text, video or pictures. Please refer to the Social Media Policy for further information.
- Staff should not post any images of staff on any social media without first obtaining permission from those person(s) in the image.

Children and young people use a variety of online tools for educational purposes. They will be asked to only use their first name or a suitable avatar for any work that will be publicly accessible and will be required to follow the principles listed above before sending any work for publishing. Staff should encourage contributions that are worthwhile and develop a particular discussion topic.

When photos and videos of Academy events are permitted to be taken by parents and carers, they will be asked not to publish them on any public area of the Internet, including social networking sites.

### **Pupil/student rules for acceptable internet use**

We will adopt the rules as laid out below in an age-appropriate way for the pupils/students at OHCAT Academies.

- *I will ask permission from an adult before using the Internet.*
- *I will use computers and tablets safely.*
- *I will not look for websites that I know I'm not allowed to see.*
- *If I see anything that I know is wrong I will tell an adult straight away.*
- *I know that I can talk to an adult if I see or experience anything on the Internet that makes me feel scared or unhappy.*
- *I will not download anything without permission from an adult.*
- *I will not use memory sticks on school computers without permission from an adult.*
- *I will ask an adult before sending emails.*

- *I will be polite and respect others when using the Internet.*
- *I will not give out any personal information over the Internet.*
- *I will not share my login details with others.*
- *I understand that the school may check my computer files and check what I am doing.*
- *I will not upload to social media any photos, videos or sound recordings that contain other pupils or staff within the academy.*

### **Visitor rules for acceptable internet use**

Visitors' Internet use will vary depending upon the purpose of their visit. Generally we expect all visitors to abide by the following rules:

- *I will respect the facilities by using them safely and appropriately.*
- *I will not use the Internet for personal financial gain, political purposes, advertising, personal or private business.*
- *I will not deliberately seek out inappropriate websites.*
- *I will report any unpleasant or upsetting material to a member of staff immediately.*
- *I will not download or install program files.*
- *I will not use USB memory devices on Academy computers.*
- *I will be polite and respect others when communicating over the Internet.*
- *I will not share my login details.*
- *I will not carry out personal or unnecessary printing.*
- *I understand that the Academy may check my computer files and monitor my Internet use.*
- *I will not make or share defamatory posts relating to the Academy on any social media.*

### **Staff and Governor rules for acceptable internet use**

Staff and governors must use the Internet safely, appropriately and professionally within the Academy. They must be aware that they are role models for others and are expected to promote and model high standards of behaviour at all times. For further details please refer to the OHC&AT IT Acceptable Use Policy.

## **E-SAFETY EDUCATION AND TRAINING**

The aim of e-safety education within OHCAT Academies is to teach pupils and students how to manage and deal with risks they encounter by themselves, whilst at the same time encouraging them to become positive users of both new and emerging technologies.

Pupils/students will be taught about safe and appropriate electronic communication, including the indelible nature of emails, social media presence, images and other e-communications. Aspects of e-safety such as cyberbullying, revenge porn, trolling and other harassment will be covered in an age-appropriate way, with emphasis placed on



respecting oneself and one's peers, in order to build confidence and understanding among pupils/students as they interact with technology.

For younger pupils/students Internet use will be closely supervised and based around pre-selected, safe websites. Pupils/students will be regularly reminded about how to always take care when clicking and to seek help from an adult if they see anything that makes them unhappy or that they are unsure about. These digital literacy skills will be developed in keeping with pupils'/students' age and ability, with lessons promoting a responsible attitude towards searching the Internet and the importance of personal security measures such as strong passwords and processes for reporting any concerns.

As they progress through the Academy, pupils/students will be encouraged to become more independent at researching information on the Internet, being taught the necessary skills to critically evaluate sites for accuracy and suitability. They will be supported to use online collaboration tools for communicating and sharing ideas.

### **E-safety updates for staff**

Staff receive regular updates about how to protect and conduct themselves professionally online and to ensure that they have an awareness of issues surrounding modern technologies, including safeguarding. Updates are delivered through CPD, staff meetings, email updates and via the staff intranet, which also signposts to relevant external resources and sources of support.

### **E-safety updates for parents/carers**

OHCAT Academies provide opportunities for parents and carers to receive e-safety education and information (e.g. via the Academy website and/or newsletters) to enable them to better understand the issues surrounding new technologies and to help them support their children in developing good e-safety.

### **Guidance on the use of social networking and messaging systems**

OHC&AT recognises that many staff will actively use Facebook, Twitter and other social networking, blogging and messaging services, including to support their own professional development by developing personal learning networks with other educational practitioners.

Staff must recognise that it is not appropriate to discuss issues relating to pupils/students or colleagues via social media networks; discretion and professional conduct is essential. Posts that bring OHC&AT into disrepute and/or breach confidentiality are likely to result in disciplinary action. Staff must review their privacy settings to make sure that their profiles and photographs are not viewable by the general public.

It is never acceptable to accept a friendship request from a child or young person in an OHC&AT provision or from ex-pupils/students who are still minors. This is to avoid any possible misinterpretation of motive or behaviour which could be construed as grooming.

Staff must not give their personal contact details to pupils/students, including e-mail, home or mobile telephone numbers. All correspondence should be via OHC&AT systems.

Please refer to the Social Media Policy, the Staff Code of Conduct and the IT Acceptable Use Policy for further details.

## DATA PROTECTION

Personal data will be recorded, processed, transferred and made available according to the principles of the General Data Protection Regulation (GDPR), which state that personal data must be:

- Processed lawfully, fairly and in a transparent manner
- Collected for specified, explicit and legitimate purposes
- Adequate, relevant and limited to what is necessary to fulfil the purposes for which it is processed
- Accurate and, where necessary, kept up to date
- Kept for no longer than is necessary for the purposes for which it is processed
- Processed in a way that ensures it is appropriately secure

Staff must ensure that they:

- At all times take care to ensure the safe keeping of personal data, minimising the risk of its loss or misuse;
- Use personal data only on secure password protected computers and other devices, ensuring that they are properly 'logged-off' or 'locked' at the end of any session in which they are using personal data;
- Be fully aware of the risks of transferring data using removable media. When personal data is stored on any portable computer system, USB stick or any other removable media, it must be securely deleted once its use is complete.

It may sometimes be necessary to send confidential information outside the organisation e.g. as part of a safeguarding investigation. **OHC&AT staff must at all times consider the security of such information.** Any confidential or sensitive information conveyed via email outside of OHC&AT systems must be encrypted. Where encryption is not available, information must be password protected and the password conveyed separately to the recipient, preferably by means other than email.

## E-SAFETY FOR PUPILS AND STUDENTS ACCESSING REMOTE OR BLENDED LEARNING

OHCAT recognises that pupils and students may experience periods where they are unable to attend school, whether due to external factors such as the ongoing coronavirus outbreak or as a result of their additional needs e.g. complex health



issues. These pupils/students will be supported to access remote or blended learning as necessary, and with appropriate safeguards in place.

When pupils/students are not able to attend school for a period of time, the risks associated with online activity including remote learning are potentially heightened. When sending work home to pupils/students currently unable to attend, Academy staff include information on staying safe online and sources of support, including reporting pathways, where students have concerns about online activity. This includes details of Safeguarding teams, as well external agencies including:

- [Childline](#) – for support
- [UK Safer Internet Centre](#) – to report and remove harmful online content
- [CEOP](#) – for advice on making a report about online abuse

Academy websites are also kept updated with relevant links and other e-safety information for both pupils/students and families.

When setting home learning, OHCAT Academies ensure any use of online learning tools and systems is in line with privacy and data protection/GDPR requirements.

OHCAT Academies operate clear procedures around delivering remote learning, including the following key points:

- Staff must adhere to the OHC&AT Staff Code of Conduct **at all times**, including when delivering remote learning.
- Ideally virtual sessions should be delivered to groups only. Where remote access is used to deliver 1:1 sessions, for example counselling sessions, these must be recorded and the recordings safely stored in accordance with OHC&AT policies on IT acceptable use and records retention. Pupils/students and parents/carers must be made aware that sessions are being recorded.
- Live group classes should also be recorded so that if any issues were to arise, the video can be reviewed.
- When planning delivery of live sessions, staff should consider the needs and profiles of each pupil/student intended to receive the session and risk assess accordingly.
- Staff and children/young people must wear suitable clothing, as should anyone else in the household.
- Any computers used should be in appropriate areas, for example, not in bedrooms; and the background should be blurred.
- Live classes should be kept to a reasonable length of time, or the streaming may prevent the family 'getting on' with their day.
- Language must be professional and appropriate, including any family members in the background.
- Staff must only use platforms specified by senior managers and approved by the IT network manager/provider to communicate with pupils/students.
- Staff should record the length, time, date and attendance of any sessions held.

Staff maintain regular contact with all pupils/students not currently attending, and this provides a further opportunity to discuss online safety with them, their parents and carers. We are aware that when a pupil/student is unable to attend school for any

length of time, families may wish to access additional home learning support, for example tutors or other specialists, and staff emphasise the importance of securing online support from reputable organisations/individuals who can provide evidence that they are safe and can be trusted to have access to children or vulnerable adults.

## **POLICY REVIEW DETAILS**

<i>Version:</i>	1.4
<i>Reviewer:</i>	James Akerman, Simon Gale
<i>Approval body:</i>	Family Board
<i>Date this version approved:</i>	2 <sup>nd</sup> July 2021
<i>Due for review:</i>	Summer 2022

## **RELATED POLICIES AND DOCUMENTATION**

Anti-Bullying Policy  
Anti-Radicalisation Policy  
Child Protection Adult Protection and Safeguarding Policy and Procedures  
Data Protection Policy and related documentation  
Dignity at Work Policy  
IT Acceptable Use Policy  
OHCAT Academies' Safeguarding & Wellbeing Offers  
Positive Behaviour Policy (Academies)  
Social Media Policy  
Staff Code of Conduct  
Student Mental Wealth, Health and Wellbeing Policy

## **APPENDIX 1: How to Stay 'Cybersafe' – Staff Do's and Don'ts**

### **DO**

- Be aware of your online reputation, which consists of information you post about yourself and information posted by others, and consider that when seeking employment, many prospective employers will use publicly available online information. Remember, the internet never forgets.
- Keep passwords confidential and protect access to accounts.
- Regularly review your privacy settings.
- Discuss expectations with friends – are you happy to be tagged in photos, for example?
- Be aware that, increasingly, individuals are being held to account in the Courts for the things they say on social networking sites.
- Keep personal phone numbers private and don't use your own mobile phones to contact pupils/students or parents/carers.
- Use an OHC&AT mobile phone for OHC&AT business.
- Keep a record of your phone's unique International Mobile Equipment Identity (IMEI) number, keep phones secure while on Academy premises and report thefts to the police and mobile operator as soon as possible.
- Ensure that Academy rules regarding the use of technologies are consistently enforced.
- Report any incident to the appropriate member of staff in a timely manner.
- Keep any evidence of an incident, for example by not deleting text messages or emails and by taking a screen capture of material, including the URL or web address.
- Use your OHC&AT email address only for work purposes.
- Be aware that if you access any personal web-based email accounts via the OHC&AT network, these may be subject to the Academy's internet protocol which could include monitoring and surveillance.
- Raise genuine concerns about your Academy or specific members of staff using whistle blowing or grievance procedures.

### **DON'T**

- Post information and photos about yourself, or OHC&AT-related matters, publicly that you wouldn't want employers, colleagues, pupils/students or parents/carers to see.
- Befriend pupils/students or other members of the school community on social networking sites. (You should consider carefully the implications of befriending parents/carers or ex-pupils/students and let the SLT at your Academy know if you decide to do this.)
- Personally retaliate to any incident or bullying messages.
- Criticise your Academy, OHC&AT, pupils/students or parents/carers online.