E-SAFETY POLICY
(Orchard Hill College)

The OHC&AT Board of Directors has agreed this Policy and as such, it applies across all OHC centres and settings – 13th December 2019.
Peter Lauener
Chair of OHC Board

E-Safety Policy (Orchard Hill College)

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 students at Orchard Hill College safe, whether using new technology in College or at home. There is a separate policy for OHCAT Academies.

This policy has been written with reference to a range of guidance including 'Teaching online safety in schools' (DfE, 2019), the 'Education for a Connected World' framework (UKCIS, 2018), the London Grid for Learning (LGfL) E-Safety Policy, the South West Grid for Learning (SWGFL) E-Safety Policy, Ofsted's Inspecting E-safety in Schools (April 2014) and the NUT Policy on E-safety. 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 cross-references to OHC&ATs Child Protection and Safeguarding Policy and Procedures. Delivering high quality e-safety education also forms part of the universal safeguarding provision detailed in the College'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 COLLEGE

Use of the Internet and other new technologies generates significant opportunities for people with learning difficulties and disabilities to enhance the accessibility of communication with friends, parents/carers, other learning providers, community activities and employers. However, there are also significant potential risks for vulnerable people when using new technology, including:

- Access to illegal, harmful or inappropriate images or other content
- Unauthorised access to, loss of, and sharing of personal information
- Internet grooming and/or 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
- An inability to evaluate the quality, accuracy and relevance of information on the internet
- Plagiarism and copyright infringement
- Illegal downloading of music or video files
- Excessive use which may impact on social and emotional development and learning

The College has a clear responsibility to recognise the benefits of new technologies and the opportunities they present, and to support our students to be able to safely navigate the digital world.

ROLES AND RESPONSIBILITIES

Orchard Hill College's Digital School works closely with the College SLT to ensure that e-safety is woven into the College curriculum. The Digital School team comprises students and staff, working together to develop digital solutions for students with SEND.

Students are able to bring their own mobile and tablet devices to College and connect them to our public wifi. The College does not accept responsibility for any damage to personal devices while at College. Teaching teams may set individual rules around when and how these devices can be used and accessed during lessons and in leisure time.

The Digital School also works to support the development and delivery of ICT through student-led digital workshops and initiatives, including annual participation in the British E-Sports tournament. Students are supported to use games appropriately and only in designated time slots. We also work with our young people around dangers of online gaming and meeting people online. We have a number of bespoke resources that The Digital School have developed to support with understanding these topics.

All College staff will familiarise themselves with this policy. E-safety is built into students' individual learning programmes and highlighted throughout the year via other opportunities e.g. as student council meetings. Staff are reminded of their e-safety obligations via regular updates, training and discussion during Inset days.

The OHC Committee has allocated a governor to hold the portfolio for Safeguarding and Child Protection. This member will monitor adherence to the policy, together with the E-Safety Lead, and feedback to the Committee as appropriate.

Orchard Hill College will monitor the impact of this policy using:

- Logs of reported incidents (maintained by the E-Safety Lead).
- Monitoring of the College network where necessary.
- Regular monitoring of the College's social media presence.
- Monitoring of the College's Google Apps platform where necessary.
- Monitoring of the College's internet access where necessary, and regular reviews of the College's website filtering.
- Student and parent/carer questionnaires.

CREATING A SAFE ICT INFRASTRUCTURE

All users of OHC&AT computer networks have clearly defined access rights, enforced using a username and password login system. Account privileges are achieved through the file and folder permissions, and are based upon each user's requirements. Students' accounts are restricted and do not allow access to all network drives. Guests are required to login 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 students)

The College website is a valuable tool for sharing information and promoting 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 student is used, they should not have their full name displayed (including in credits).
- Staff **must not** take photographs of students using their personal devices – all student photographs must be taken using OHC&AT equipment.
- Files should be appropriately named in accordance with these principles.
- Only images of students in suitable dress should be used and group photographs are preferred (though not exclusively) in preference to individual photographs.
- Students and parents/carers are given the opportunity to withdraw permission for the College to publish images/audio/video of a student on the College 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 proofread by a member of the College's Senior Leadership Team before being published.

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.

Student guidelines for acceptable internet use

Students are expected to use the Internet responsibly, safely and within the parameters of the IT Acceptable Use Policy. Staff will work with students to support safe and appropriate Internet use, as part of each student's individualised learning programme.

Student use of social media

Social media is an established and growing phenomenon. Many of our students already access social media outside of College, or are interested in doing so, and there are many potential benefits, including increased opportunities to communicate and socialise.

The College will support students to access social media safely. Ways we will do this include:

- Supporting students to use Sharespace, the purpose-built safe social network created by Orchard Hill College, and using this as a springboard to build safe social networking habits.
- Giving clear direction on what to do if students have concerns about inappropriate material or contacts, e.g. raising concerns with parents/carers or other trusted adults and with College staff, exploring resources such as www.saferinternet.org.uk
- Using applications such as Facetime or Skype, where students can see who they are communicating with, as teaching tools.
- Giving students the opportunity to explore issues around cyberbullying and appropriate social behaviour online.

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 College 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 College may check my computer files and monitor my Internet use.*

Staff and Governor rules for acceptable internet use

Staff and governors must use the Internet safely, appropriately and professionally within the College. They must be aware that they are role models for others and should 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 College promotes safe use of technology and ensures that use of ICT is embedded throughout the curriculum. Upon enrolment at Orchard Hill College each student has a digital portfolio, Sharespace account and E-Learning assessment. The digital portfolio allows a student to interact with their curriculum and control what they say about their learning journey. Sharespace is a bespoke social network that teaches students about online safety whilst using social media. This not only promotes and teaches e-safety but also enhances interactions between students and gives them a platform to speak up and be heard. Our assessments are rigorous and pinpoint what resources and learning materials a student will require in order to fully access our curriculum.

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. They are also directed to relevant websites to help support their understanding of these issues. Some of this information will be provided by email updates and at staff meetings.

E-safety updates for parents/carers

OHC&AT aims to work with parents and carers to help them support their children's education and achievement. Parents/carers of College students are encouraged to contact the College at any time if they have concerns about e-safety or would like further information on supporting e-safety practices in the wider world.

Guidance for staff 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 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 should 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-students. 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 students, including e-mail, home or mobile telephone numbers. All correspondence should be via OHC&AT systems.

Please refer to the Staff Code of Conduct 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.

POLICY REVIEW DETAILS

Version:	1.2
Reviewer:	Kelly Phillips, Simon Gale
Approval body:	Family Board
Date this version approved:	13th December 2019
Due for review:	Autumn 2020

RELATED POLICIES AND PROCEDURES

Anti-Bullying Policy
Anti-Radicalisation Policy
Child Protection Adult Protection & Safeguarding Policy and Procedures
Data Protection Policy
Dignity at Work Policy
IT Acceptable Use Policy
Orchard Hill College Safeguarding & Wellbeing Offer
Positive Behaviour Policy (Orchard Hill College)
Staff Code of Conduct
Student Mental Wealth, Health & 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 OHC&AT premises and report thefts to the police and mobile operator as soon as possible.
- Ensure that OHC&AT 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 OHC&AT's internet protocol which could include monitoring and surveillance.
- Raise genuine concerns about an OHC&AT provision or specific members of staff using whistle blowing or grievance procedures.

DON'T

- Publicly post information and photos about yourself, or OHC&AT-related matters, that you wouldn't want employers, colleagues, pupils/students or parents/carers to see.
- Befriend pupils/students or other members of the school/College 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 place of work know if you decide to do this.)
- Personally retaliate to any incident or bullying messages.
- Criticise your place of work, OHC&AT, pupils/students or parents/carers online.