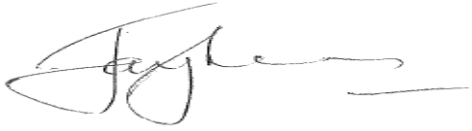
IT ACCEPTABLE USE POLICY

The OHC&AT Board of Directors has agreed this Policy and as such, it applies across the organisation – 15th December 2017.

Jay Mercer
Chair of OHCAT Board



Darren Coghlan
Chair of OHC Board

IT Acceptable Use Policy

INTRODUCTION

Orchard Hill College and Academy Trust (OHC&AT) is committed to providing outstanding educational opportunities for all our pupils and students. OHC&AT recognises that successful support for pupils and students is wholly dependent upon the ethos of the organisation. It is incumbent on the whole OHC&AT community to promote positive behaviour and maintain a positive regard towards pupils/students and colleagues.

This policy covers the security and use of all OHC&AT information and IT equipment. It also includes the use of email, internet, voice and mobile IT equipment. This policy applies to all OHC&AT employees, contractors and agents (hereafter referred to as 'individuals').

This policy applies to all information, in whatever form, relating to OHC&AT's organisational activities worldwide, and to all information handled by OHC&AT relating to other organisations with whom it deals. It also covers all IT and information communications facilities operated by OHC&AT or on its behalf.

AIMS AND OBJECTIVES

All IT facilities and information resources remain the property of OHC&AT and not of particular individuals, teams or departments. Adherence to this policy will help ensure that IT equipment is used:

- Legally
- Securely
- Effectively
- Without undermining OHC&AT
- In a spirit of co-operation, trust and consideration for others
- In a way that ensures the equipment remains available

The policy relates to all Information Technology facilities and services provided by OHC&AT IT Shared Services. All staff, volunteers and contractors are expected to adhere to it. This policy should be read in conjunction with the Computer Misuse Act 1990 as well as the Data Protection Act 1998.

It is your responsibility to report suspected breaches of security policy without delay to your line manager and/or the IT department. All breaches of information security policies will be investigated. Where investigations reveal misconduct, disciplinary action may follow in line with the OHC&AT Disciplinary Procedure.

The OHC&AT IT team holds overall responsibility for OHC&AT IT equipment. You should not rearrange IT equipment (computers, power supplies, network cabling, modems etc.) without first contacting OHC&AT IT staff. Additionally, any damage, loss or theft of OHC&AT IT equipment must be reported to OHC&AT IT staff immediately.

Staff are discouraged from using personal IT equipment e.g. smart phones to conduct OHC&AT business. In particular, staff **must not** take photographs of pupils or students on their personal devices. Any personal devices that are used for OHC&AT business should be appropriately secure e.g. password/PIN protected, and should not be used for storing OHC&AT data. Please contact the OHC&AT IT department for further details.

CONFIDENTIALITY

It is the responsibility of all staff to maintain appropriate confidentiality across the organisation.

All information relating to pupils and students obtained by any individual working for OHC&AT is confidential to the organisation. Such information must not be disclosed to anyone outside the organisation without the informed consent of a line manager.

Confidentiality also applies to other aspects of OHC&AT operation. This includes but is not limited to:

- Accounts information
- Technical information
- HR information
- Marketing and sales information
- Pricing information

The non-authorised photographing, recording or copying of confidential information belonging to pupils/students and other stakeholders by using, for example, computers, phones, cameras or memory sticks, may be considered a breach of confidentiality.

OHC&AT will regard any breach of this confidentiality agreement as a disciplinary offence and serious breaches may lead to dismissal without notice for gross misconduct.

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 must be password protected and the password conveyed separately to the recipient, preferably by means other than email.

COMPUTER ACCESS CONTROL

Access to OHC&AT IT systems is controlled by the use of User IDs and passwords. All User IDs and passwords are uniquely assigned to named individuals and consequently, individuals are accountable for their actions on OHC&AT IT systems.

You must:

- Always lock or log off your PC when leaving it unattended. You are responsible for any misuse of your PC that might occur as a result of not following this rule.

- Ensure you are not breaking data protection legislation if/when you record or obtain information about individuals. Please refer to the Data Protection Policy for further details, or speak to your line manager or a member of the OHC&AT IT team.

You must not:

- Allow anyone else to use your user ID and password on any OHC&AT IT system.
- Leave your user account logged in at an unattended and unlocked computer.
- Use someone else's user ID and password to access OHC&AT IT systems.
- Leave your password unprotected (for example by writing it down).
- Perform any unauthorised changes to OHC&AT IT systems or information.
- Attempt to gain unauthorised access to information or facilities.*
- Store OHC&AT data on any non-authorised OHC&AT equipment.
- Give or transfer OHC&AT data or software to any person or organisation outside OHC&AT without the authority of OHC&AT.

By default, and with the exception of approved devices, access to external hard drives such as USB keys, camera cards and other devices containing SD Cards is blocked via OHC&AT security software. You should contact the IT department for device approval or for assistance with copying data from these types of device.

**The Computer Misuse Act 1990 makes it a criminal offence to obtain unauthorised access to any computer (including workstations and PCs) or to modify its contents. If you don't have access to information resources you feel you need, speak to your line manager or the OHC&AT IT department.*

INTERNET AND EMAIL CONDITIONS OF USE

Use of OHC&AT internet and email is intended for business use. Personal use is permitted where such use does not affect the individual's business performance, is not detrimental to OHC&AT in any way, not in breach of any term and condition of employment and does not place the individual or OHC&AT in breach of statutory or other legal obligations.

You are accountable for your actions on the internet and email systems. Your 'virtual self' is as much a representative of OHC&AT as your physical self. When you're on the internet and/or using email you must:

- Always assume everyone will read everything you write.
- Make sure your actions are in the interest and spirit of OHC&AT and ensure that you don't write anything that could be deemed as bringing OHC&AT's good name into disrepute. Any action that is deemed to be in breach of the above may result in disciplinary action being taken against you.

You must not:

- Use the internet or email for the purposes of harassment or abuse.
- Use profanity, obscenities, or derogatory remarks in communications.

- Access, download, send or receive any data (including images), which OHC&AT considers offensive in any way, including sexually explicit, discriminatory, defamatory or libellous material.
- Use the internet or email to make personal gains or conduct a personal business.
- Use the internet or email to gamble.
- Use the email systems in a way that could affect its reliability or effectiveness, for example distributing chain letters or spam.
- Place any information on the internet that relates to OHC&AT, alter any information about it, or express any opinion about OHC&AT, unless you are specifically authorised to do this.
- Send unprotected sensitive or confidential information externally.
- Forward OHC&AT mail to personal (non-OHC&AT) email accounts (for example a personal Hotmail account).
- Make official commitments through the internet or email on behalf of OHC&AT unless authorised to do so.
- Download copyrighted material such as music media (MP3) files, film and video files (not an exhaustive list) without appropriate approval.
- In any way infringe any copyright, database rights, trademarks or other intellectual property.
- Download any software without prior approval of the IT Department.
- Connect OHC&AT devices to the internet using non-standard connections.

The OHC&AT email system shall not be used for the creation or distribution of any disruptive or offensive messages, including offensive comments about race, gender, hair colour, disabilities, age, sexual orientation, pornography, religious beliefs and practice, political beliefs or national origin. Employees who receive any emails with this content from any OHC&AT employee should report the matter to their line manager immediately.

EMAIL SECURITY AND ETIQUETTE

Security

If your email contains sensitive or confidential material (i.e. contains personal details of an individual, is confidential or contains information that should not be shared with any other person), ensure you send any confidential/sensitive details in a secure format, preferably encrypted. If encryption is not available, you should send a password-protected Word document attached to the email and communicate the password to the receiver via text or verbally.

- Do not use simple passwords.
- Do not share your password with another individual and always log off the system when you have finished working on your computer/laptop/tablet
- Do not insert details of an individual in the subject field of an email. Keep your subject title generic to the content without being too specific.

Etiquette

Write carefully. Once you send an email, you cannot take it back or make it disappear. The reality is that your messages may be saved for a very long time. They may also be read inadvertently by others, used to provide evidence in employment cases, or forwarded to others without your knowledge.

Be courteous. Use upper and lowercase text, left justified. Using all uppercase letters gives the impression of SHOUTING. Most people find it annoying and those who are visually impaired can find capitals and fully justified text harder to read.

Be aware. Emails may convey a difficult or sensitive message in a light that was not necessarily intended. A written message could be misunderstood by the recipient. Difficult messages are better given face to face.

Be diplomatic. Criticism is always harsher when written, and email can be easily forwarded.

Be calm. You may have misunderstood what was meant. Don't reply if you're angry.

Be brief. Don't include background images, pictures, animations, etc. unless they are critical to your message.

Be precise. Address your messages carefully. Some addresses may belong to a group, even though the address appears to belong to just one person.

What not to do

Do not get fooled by Internet hoaxes and computer virus myths.

Do not forward a so-called virus alert to everyone you know – instead report the email to the IT Helpdesk and delete the message.

Do not forward emails unless you are certain it is agreeable to the sender. Gain permission from the author if necessary.

Do not respond to an email unless a response is requested from the sender or they have particularly gone out of their way to help you, in which case you may wish to thank them for their services.

Don't forget – people can receive a high volume of emails. It is often quicker and easier to communicate with a telephone call.

REMOTE ACCESS

It is the responsibility of OHC&AT employees, contractors, vendors and agents with remote access privileges to OHC&AT's IT system to ensure that their remote access connection is given the same consideration as the user's on-site connection to OHC&AT.

It is your responsibility to manage your remote access to the OHC&AT network in accordance with this policy in the same way as on-site access e.g. protect your password, do not leave your workstation unlocked and unattended etc.

Additionally, the following controls must be applied:

- Equipment and media taken off-site must not be left unattended in public places and not left in sight in a car.
- Laptops must be carried as hand luggage when travelling.
- Information should be protected against loss or compromise when working remotely (for example at home or in public places). Laptop encryption must be used.
- Particular care should be taken with the use of mobile devices such as laptops, mobile phones, smartphones and tablets. They must be protected at least by a password or a PIN and, where available, encryption.

SOFTWARE

Employees must use only software that is authorised by OHC&AT on OHC&AT computers. Authorised software must be used in accordance with the software supplier's licensing agreements. All software on OHC&AT computers must be approved and installed by the OHC&AT IT department.

In-house software (software written by staff or volunteers using OHC&AT equipment) is the property of OHC&AT and must not be used for any external purpose. Software developers (and students) employed by OHC&AT are permitted to take a small portfolio of such in-house software source code/executables, which they may have developed, for use in subsequent work, subject to written agreement by the IT Manager and the Principal/CEO.

You must not:

- Store personal files such as music, video, photographs or games on OHC&AT IT equipment.

VIRUSES

The IT department has implemented centralised, automated virus detection and virus software updates within OHC&AT. All PCs have antivirus software installed to detect and remove any virus automatically.

You must not:

- Remove or disable anti-virus software.
- Attempt to remove virus-infected files or clean up an infection, other than by the use of approved anti-virus software and procedures.

TELEPHONY (VOICE) EQUIPMENT CONDITIONS OF USE

OHC&AT voice equipment is intended for business use. You must not use OHC&AT voice facilities for sending or receiving private communications on personal matters, except in exceptional circumstances. All non-urgent personal communications should be made at your own expense, using alternative means of communications.

You must not:

- Use OHC&AT voice equipment for conducting private business.
- Make hoax or threatening calls to internal or external destinations.
- Accept reverse charge calls from domestic or international operators, unless it is for business use and you have prior authorisation to do so.

ACTIONS UPON TERMINATION OF CONTRACT

All OHC&AT equipment and data, for example laptops and mobile devices including telephones, smartphones, USB memory devices and CDs/DVDs, must be returned to OHC&AT at termination of contract.

All OHC&AT data or intellectual property developed or gained during the period of employment remains the property of OHC&AT and must not be retained beyond termination or reused for any other purpose.

MONITORING AND FILTERING

Any information available within IT facilities may be monitored for safety and safeguarding purposes. This may include; monitoring employees' working activity, working time, files accessed, Internet sites accessed, reading of their email or private files etc. Monitoring is carried out by automated collection and alerting systems and the information is not viewed without prior authorisation.

Exceptions will be made:

- In the case of a specific allegation of misconduct – the IT Manager can authorise accessing of such information when investigating the allegation. The subject of the allegation may have their access to IT facilities disabled, pending investigation.
- When IT Shared Services cannot avoid accessing such information whilst fixing a problem – in such instances, the person concerned will be informed immediately and information will not be disclosed wider than is absolutely necessary.
- In the case of automated systems used for monitoring and alerting of possible breaches of policy or security. The IT department have various automated systems that will alert the IT Management team if a possible issue has arisen, following which further investigation can then take place. All email, file server and web access is monitored by automated systems.

Any monitoring will be carried out in accordance with audited, controlled internal processes, the UK Data Protection Act 1998, the Regulation of Investigatory Powers

Act 2000 and the Telecommunications (Lawful Business Practice Interception of Communications) Regulations 2000.

POLICY REVIEW DETAILS

Version:	1.2
Reviewer:	Janet Sherborne, Stephanie Hill
Approval body:	Family Board
Date this version approved:	15th December 2017
Due for review:	Autumn 2020

RELATED POLICIES AND PROCEDURES

Child Protection, Adult Protection and Safeguarding Policy and Procedures
Data Protection Policy
Dignity at Work Policy
E-Safety Policy
Staff Code of Conduct