HIGHCLIFFE SCHOOL

INFORMATION AND COMMUNICATION TECHNOLOGY ACCEPTABLE USE POLICY (AUP)

Drawn up by:	Harry Glyde, Senior IT Technician
Date:	14th May 2020
Date adopted by Governing Body:	14th May 2020
Review Date:	May 2022

1 Introduction

This policy sets out the acceptable use of Information and Communication Technologies within Highcliffe School. Copies of this document are available on the school website.

2 Definition of Terms

The following terms are used in this document and relate to the following:
Network User – any person that uses the school's network infrastructure.
Staff – any employee of the school or visiting consultant, adviser or other visitor to the school.
Student – any person who attends the school for education purposes.
Hacking – any attempt to bypass any of the school network's security or filtering systems.
The School – Highcliffe School. AUP – Acceptable Use Policy.
VLE/FLE – the school's flexible learning environment (MyHighcliffe).
Laptop/Device/iPad/Tablet/Computer – these terms are used interchangeable and refer to a connected electronic device.

3 School-wide policies and procedures

The School's Acceptable Use Policy (AUP) is part of a suite of documentation which covers the safe and legal use of ICT within the school. These include (but are not limited to) child safety, anti-bullying, health and safety, data protection act, GDPR, CCTV, fair processing, mobile phone, social networking and copyright.

Use of ICT is monitored within the school, and cases of misuse by staff and students will be reported to the Headteacher. A log of any incidents is kept on the student information system or in staff files. The AUP will be reviewed annually, and action taken if a need for change is identified.

Where our filtering system detects attempts to access websites or materials considered to present a risk of harm (including, but limited to intolerance, racism, terrorism and self-harm) will automatically generate an alert that will be sent to the School's Safeguarding team as part of our statutory duty to monitor access. The school may also share our filtering reports with external services to help us identify inappropriate or safeguarding issues.

4 Communication with parents and carers

Parents are contacted directly where concerns exist regarding improper use of the Internet or school's ICT equipment. Improper use may result in students being banned from using systems and other disciplinary measures may be taken depending upon the nature of the abuse (e.g. Exclusion from school). All misuse and IT related issues will be dealt with under the school Behaviour Policy

All emails/communication/documents/etc. must be thought through and entirely professionally worded.

5 Acceptable use guidelines for staff

Any school computer equipment or service utilised by a member of staff is provided for the primary purpose as a work tool, for work related duties only. It must not be used to conduct a personal business/enterprise for personal gain or to access/store any information/media/photos/files that could be seen to be inappropriate on the device. Any electronic communication with other members of the school must be made using the internal school systems taking into account that all communication/files must be of a professional nature.

Staff must keep their passwords secure and make sure their passwords are of significant strength. They must include a mixture of upper case, lower case and numbers to make it difficult for anyone to guess. Passwords must not be given to any other members of staff or students at any time and care must be taken when typing in passwords to a device/computer/laptop to make sure that no other person can identify the password or pin code.

Staff are responsible for the security and acceptable use of their laptop/device/network account. Staff must ensure that their laptop and other computer equipment is stored securely when not in use. Staff must not keep passwords with their laptop. If a laptop is lost or stolen, a report must be made to the Police. Staff must provide the Police with a phone number for IT Support so that the equipment's serial number can be provided. IT Support must be provided with the crime reference number for insurance purposes.

Laptops store their files on their own internal hard discs which require backing up to the network on a periodic basis. The system will remind the member of staff when this is due but it is the responsibility of the member of staff to make sure this is carried out. Should a hard disc fail and no recent backup exists IT support may not be able to rescue lost files. In relation to personal devices such as smartphones or tablets, any important documents should be emailed to your own account or stored on their school provided cloud storage (OneDrive or Google Drive) to keep them safe should the device fail.

Staff are expected to maintain reasonable care with all portable equipment. This includes taking measures

to ensure that the equipment is transported in a safe and secure manner. Staff should be aware that all portable equipment is insured whilst in school or at home via the school's insurance where forced entry can be proven. The school's insurance does cover equipment which is left unattended in a motor vehicle as long as:

a) the property insured is concealed in a glove compartment or locked luggage compartment; and

b) all doors are locked; and

c) all windows and the roof are closed and fastened; and

d) all security devices are put in full and effective operation; and

e) all keys or any other removable ignition device of the vehicle are removed

Staff must not keep 'personal information' about students on their laptops in case of theft – data such as contact details etc. should not be stored on laptops.

All software should be installed by IT Support and must have the relevant license made available to them before installation. Software without the correct license must not be installed and staff who attempt to install
software themselves will be responsible. With mobile devices and Apps if you require a password to install the app this must be carried out by IT Support (some devices may be unlocked to allow you to undertake this yourself).
Online learning systems (such as Kerboodle or Accelerated Reader) and all other software packages should be approved by the IT Support team before being purchased or set up.

IT Support maintains a software audit, containing a list of the software installed on each computer or laptop. This audit will be made available to any official body who require it for the purposes of copyright enforcement. The use or copying of software without the licensor's permission is illegal and equally the terms and conditions of software licenses must always be adhered to.

The copying of music files, video and other copyright material if not legally purchased by the member of staff/students onto school computers may be illegal and removed if discovered. DVDs and media from online streaming services such as YouTube, Netflix and Amazon Prime Video may only be played to an audience if it is within the terms of their license agreement or the school holds an additional license which allows. School mobile devices may be locked to not allow such content in which case no member of staff should circumvent this setting.

Whilst it is the user's responsibility to take reasonable care over the configuration of their computer hardware, it is possible for software to be installed on a machine without the full comprehension of the user. Users discovering software that has been installed in an unsolicited manner and which contravenes the licensing regulations above must contact IT Support who will assist in resolving any issues.

The school has the right to seize/reclaim any laptop or computer without explanation.
IT Support have the ability to view all files on the network and devices but are prohibited from doing so without permission from the Headteacher, Chair of Governors or the Senior IT Technician.
Staff are responsible for backing up data when they end their employment with the school. Staff must be aware of the Data Protection Act and are prohibited from taking copies of any personal data about students or other members of staff.

Any electronic contact with Parents/Guardians will follow the schools communications protocol. This means alternative methods may be used and that any communication timescale will reflect workload and wellbeing of our staff. Any contact with students via electronic means must be for the purpose of teaching and learning only and must only be carried out via the school's own systems (e.g. School email or VLE/FLE system) – this includes not sending emails to student personal accounts and only sending mails to their school email addresses.
No use of personal email/social networking systems/mobile messaging etc. should ever be used to communicate with students of the school for child protection and staff protection (e.g. allegations against a member of staff etc.). Staff are required to make themselves aware of the school's social networking policy.

All emails/communication/documents/etc. must be thought through and entirely professionally worded.

Staff should also follow the Acceptable use Guidelines for Students as detailed in Section 6 and against the safe use guidelines in section 10.

6 Acceptable Use Guidelines for Students

Students:

- Must only use the own user area and not attempt to access other users' files.
- Must keep their passwords secure and make sure no one else knows it. Passwords should not be easy to guess.
- May only use the computers/devices for school work or Home Study.
- May use flash drives or other media if installed on the computers, but only for purposes of transferring or

saving their work.

- Must only send e-mails/messages to people known to themselves or with the permission of a member of staff.
- Must only send e-mails/messages that are polite and responsible and must not contain any personal information about themselves.
- Must report any damage of equipment to a member of staff immediately.
- Must only use the school email/messaging system for school related messages.
- Must report to a member of staff any inappropriate messages they have received. All information will be treated in the strictest confidence.
- Must report to a member of staff any inappropriate website, image or video clip if they discover one is accessible from the school network.
- Are subject to checks of their computer and Internet usage. E-mails/messages may also be monitored.
- If students fail to abide by the above conditions, their Internet access may be blocked at the discretion of a senior member of staff. In severe cases network access may be removed.
- Must not attempt to breach the school's network security, intrude into other peoples 'e-space' or attempt to take the identity of another user (e.g. use another students username).
- Students must not contact staff via any 'personal systems' such as texting a member of staff or sending a message to a member of staff's personal account. Students can view the school's social network policy via the school website.

7 Data Protection Act

Data is stored in accordance with the regulations laid out by the Data Protection Act. We will take every reasonable precaution to protect information. Appropriate physical, electronic and procedural safeguards are in place to ensure the security, integrity and privacy of all information kept in our MIS. The need for confidentiality will be respected, and sharing of data will only occur with the express permission of parents/carers in line with our fair processing notification. All 'personal data' will only be allowed out of the school with the knowledge of the Headteacher, Senior IT Technician and Data and Examination Manager. Full details including our GDPR data map can be found on our website at highcliffe.school/GDPR.

8 Internet safety skills development for students

Internet safety skills are introduced to all students in Year 7 through a teaching unit designed for this purpose. This is reinforced by a second unit in Year 8. Students receive follow up lessons in 9, 10, 11 via their studies and external visitors/briefings. Students are made aware through ICT and Citizenship/PSHE of their rights and responsibilities with regard to their use of technology. This includes issues such as cyber bullying, personal safety, data security and sexting.

9 Personally Owned Equipment

Students may bring personally owned equipment (Laptops, Cameras, Tablets etc.) into school but must be aware that they are not covered by the school's insurance and are brought into school at the owner's risk. If personally owned equipment is brought into school it is down to the member of staff in charge as to when/if the equipment is

allowed to be used within lesson time. Students must seek the permission of the member of staff in charge of the class before using the equipment. Should equipment use be abused or inappropriate use be discovered within school, the students right to bring in such equipment into school may be revoked and disciplinary sanctions may be used dependent upon the nature of the abuse.

If personally owned equipment is used within school it should not be used to make recordings (video and/or sounds) of others if the other parties permission has not be sought prior to the recording.

The school reserves the right to confiscate any such equipment and it will be held securely until a parent/guardian is able to pick up the equipment from school. Any personally owned equipment must be used in accordance to this acceptable use policy.

Such equipment may be placed onto the school's 'Bring Your Own Device' (BYOD) wireless network but will need to have adequate and automatically updating virus protection/security software.

Students should be aware that the internet traffic and of devices connected to BYOD wireless network will be monitored (and alerts may be sent to relevant staff) and logged for the duration of the connection. (see 10.1)

Students should be aware that any work undertaken on non-school equipment or stored on memory sticks (or other removable media) is not backed up by the school system. Students must ensure they take adequate steps to back up their work to prevent loss of work and particularly any vital coursework.

10 Using the technologies safely

All users of the school's systems (staff and students) must be aware that any electronic communication or document is open for public access/accountability and scrutiny via such legislation as the Freedom of Information Act.

All emails/communication/documents/etc. must be thought through and entirely professionally worded.

10.1 Internet

All Network Users must use their own network account to logon to the network. The School's auditing software automatically records the address of all websites accessed and this information can be retrieved by IT Support. All Internet access is filtered by the school's Smoothwall system. Despite all reasonable steps being taken, if an unsuitable content is discovered, this should be reported immediately to a member of staff or IT Support. Attempts to bypass the filtering system are strictly prohibited and may result in a user's Internet access being removed. All access matching safeguarding criteria is reported daily to a member of the safeguarding team. IT Support have access to unfiltered access for testing purposes and its use is governed by this AUP. Use of the unfiltered access must be sanctioned by the Senior IT Technician.

10.2 Email and Messaging

All Staff and Students have an individual email account. All Network Users must use their school email account for all school related correspondence. Staff should be aware that, where necessary, their email account may be monitored by the Senior IT Technician. Staff should immediately report any inappropriate emails they receive to the Headteacher or IT Support. IT Support may be involved in extracting emails from the server.

Students and staff should be aware that their school email account may be monitored, either randomly or where any suspicion has arisen. The random monitoring of the accounts will be done by IT Support or senior staff.

Where suspicion has arisen, the Senior IT Technician will be responsible for reviewing the emails, and IT Support may be involved in extracting the emails from the server.

The school's email system will monitor against a set of banned words for any messages including these words being 'referred' until either accepted or rejected by IT Support.

10.3 Webmail

Webmail is available via the school's email system, enabling users to access their email account from any device with Internet access. The webmail is a publicly accessible website and as such users must ensure that they have strong passwords in place to protect against unauthorised access.

10.4 Spam and Spoofing (Phishing etc)

The School uses the Microsoft Exchange Online Protection mail filtering service. This service reduces the amount of malicious, spam and spoofing emails but users should still be aware on how to recognise malicious, spam and spoofing or phishing emails and delete them immediately without opening them.
Malicious emails will either contain attachments or links containing malicious code that will attempt to steal data, lock access to the device or files and demand ransom (ransomware such as cryptolocker), or install other malicious software onto the network or devices.
Spam refers to unsolicited email – email that is sent without your permission, usually offering medication or other products such as computer software at lower prices. The subject of a spam message is usually designed to attract people to reading it and therefore you may see subjects such as 'Hot Stock Notice' or 'OEM Software'.
Spoofing and Phishing refers to an email which claims to be from a bona fide company, such as a bank, requesting that you visit 'their' website and confirm your details. Email subjects will often be similar to 'Regarding Your Online Account' or 'Confirm Your Internet Banking Records'. These sites do not belong to the company they claim to be from and subsequently use your details to access your bank account. A genuine organisation would never ask you to confirm details in such a manner.

10.5 Social Networking Sites and Chat Rooms

Staff and Students should not access social networking sites or chat rooms on the school network unless these systems are owned and or managed by the school (e.g. The school's VLE\FLE system, Google Classroom or Microsoft Teams).
Should Staff or Students wish to set up a social networking site or visit a chat room (or similar) in their own time outside of the school's IT system, they must ensure they do not give away any personal information, such as their address. For their own protection, the school would like to remind all students to never upload a photo along with their full name or personal details such as which school they attend.
The School regularly monitors websites to discover any inappropriate material about the School, Staff or other Students and will take appropriate action where

necessary. Students and Staff should make themselves aware of the school's Social Networking Policy which is available on the school website.

10.6 Instant Messaging

Student users are unable to install such software and the use of websites offering an alternative are not to be accessed.

10.7 Webcams

Where video conferencing/webcams are used within school, it must be with an authorised third party and overseen by a member of staff and only if the students involved have the relevant media permissions obtained. If webcams are used within school, it should be with permission of the member of staff in charge and should never be used to record people if they are unaware of the recording.

Staff and Students should be aware that certain viruses and Trojans do exist which can activate a webcam without the owner's permission.

10.8 Peer-to-Peer (P2P) Networks

Staff and Students are forbidden from connecting to and/or downloading data from peer-to-peer networks. Peer-to-Peer networks (such as Bit Torrenting, LimeWire, BearShare or Morpheus) often contain copyrighted content, viruses, spyware or other inappropriate materials and users should be aware that downloading torrents, and files from a Peer-to-Peer network may be illegal or compromise their computer.

11 School websites

The school has its own website. It is the responsibility of the Senior IT Technician to ensure that all materials on the school website do not infringe the intellectual property rights of others. The Senior IT Technician will take all reasonable steps to ensure that material created by the school is protected under copyright. The Senior IT Technician will ensure that the website is regularly checked for inappropriate content or material and that access to the website server is secured by a strong password to prevent unauthorised access.

The school cannot be held responsible for the content of external sites, even if they are linked to from the school website.

12 Use of Student Photographs & Video

Students will have their photographs taken both formally (by school photographers and for use on the school's information systems) and informally (for example trips/visits or around school during activities). If photos are to be used for media/website/publications/newsletters then parental permission must be sought.

Parents are asked for permission when students enter the school and yearly with information update forms. Students that have no permission or have 'exclusions' (such as not using on the web etc.) can be identified via the Photograph Permission Applet from within SIS, or by hovering over the media issue icon in the group view of SIS. If exclusions exist or permission is denied then contact should be made with the parent to seek permission – if permission is not given in writing (form available from Exams and Data office) then the photo must not be used.

Videos of students working may be taken by staff for internal feedback use or for assessment purposes to be sent to examination bodies, these recordings will not be made publicly available.

Parental Permission is required even for students that are over 18 years old.

Appendix i

ICT Use Frequently Asked Questions

Introduction

The purpose of this frequently asked question sheet is to give generic examples of acceptable and safe use of the school's ICT systems in accordance with the school's ICT policy. If at any point you are unsure as to what is acceptable or safe then please contact the school's IT support office who can advise.

Q: **A student has emailed me from their own personal email address (eg. Hotmail, Googlemail). Can I respond to that email address?**

A: **You should reply to that student's school email account (ending in @highcliffe.dorset.sch.uk or @highcliffeschool.com or @highcliffe.school) and not enter into communication using the external system.**

Q: **A student has asked me to be their 'friend' on Facebook (or other social network/online gaming system – Xbox etc). Can I accept them?**

A: **No – you should not make contact with students via any social networking site or messaging system (such as Whatsapp, Instagram, text messaging, etc). Any such contact should be reported to the Senior IT Technician or Headteacher so follow up can occur with the student (via HOA etc). You should also read the school's social network policy which is available from the school website.**

Q: **Can anyone request my communication/files/messages? Do I need to keep my communication/files/messages professional at all times?**

A: **Yes - All users of the school's systems (staff and students) must be aware that any electronic communication or document is open for public access/accountability and scrutiny via such legislation as the Freedom of Information Act. All emails/communication/documents/etc. must be thought through and entirely professionally worded.**

Q: **Students are doing a presentation from my laptop/device and need my password to logon/remove screensaver. Can I give it to them?**

A: **No – your password has access to highly sensitive information and must be kept secure. Passwords must include a mix of uppercase letters, lowercase letters and at least one number to make sure they are secure. Care must be taken that when entering your password/passcode/pin that no other person is watching to try and obtain it for later use.**

Q: **I have been asked by an external contact/agency to provide them with a list of students in a year group.**

Can I send them this information?

A: **No – any personal information going to external parties must be agreed by the Headteacher or the Senior IT Technician. Information is protected under the Data Protection Act and our fair processing notice (on school website). The school must have regards to this before transferring information to any external party.**

Q: **A parent has emailed me and I need to respond. Can I email them back?**

A: **Yes – you can reply to an email from a parent but should follow the School's communications protocol when doing so. All emails/communication/documents/etc. must be thought through and entirely professionally worded.**

Q: **Can I take my laptop/tablet/device home?**

A: **Yes – you can take it home and join it to your own internet connection if desired. However, the laptop/tablet/device is for school use and must not be used to conduct a personal business/enterprise for personal gain (tax implications may exist). The laptop/tablet/device must be transported securely and safely. Insurance will only cover the laptop it is locked away out of sight when transported. Where a device has been locked by IT support no attempt should be made to circumvent the security in place. You must make sure that the device is not used to access any illegal or inappropriate content when connected to your own internet connection – if any such content is discovered this will be referred to the Headteacher who is likely to enact the school's disciplinary procedures (staff and students)**

Q: **Who is responsible for backing up my laptop/device?**

A: **You – on a laptop to do this go into Highcliffe Shortcuts on your desktop and find the link to Backup Laptop. This will store the files on a school server. Laptop drives do go wrong and IT support can only get back what exists on your last backup. Staff must ensure that they do this regularly. If you have important files on other devices (mobiles/tablets etc) please regularly email these documents to your school email account or upload to one of your school provided cloud storage areas to keep a copy off the device.**

Q: **I am working with a student and they could benefit from using my device. Can they do this?**

A: **When working directly with students they can use your device but only under your direct supervision so you can ensure that they do not use the device to access anything they should not view such as your email or an area of the network that is only for staff.**

Q: **Can I install my own software (personally owned or purchased) on to my laptop/device?**

A: **You must seek permission from the IT Support – if you wish to have software installed that the school owns then please visit IT support. For iPads/Tablets/Apps requests for installation can be made to IT Support who will evaluate the app against the cost and arrange installation if deemed acceptable.**

Highcliffe School
11-18 Academy

Appendix ii – Laptop/Device Loan Agreement

Highcliffe School Staff Device Loan agreement.

Device Make:
Model:
Serial Number:
Asset Number:
Device Name:
Date: 15/05/2020

The laptop/device detailed above is loaned to for the duration of their employment at Highcliffe School subject to the following terms and the schools ICT policy. The laptop/device must be returned to the school on ceasing to be employed at the school or if required during a planned absence.

1. The laptop/device is for the work related use of the named member of staff to which it is issued.

2. Only software installed at the time of issue or software purchased by and licensed to Highcliffe School may be installed on the machine.

3. The laptop/device remains the property of Highcliffe School throughout the loan period. However the member of staff to which it is issued, will be required to take responsibility for its care and safe keeping.

4. The laptop/device is covered by Highcliffe School Insurance, when at home or school, providing it is not left unattended. If left unattended for a short period in a car it is placed in a locked boot out of sight.

5. If left unattended the laptop/device should be in a locked room or secure area.

6. Due regard must be given to the security of the computer if using other forms of transport.

7. In order to ensure the schools compliance with the Data Protection Act and to avoid breaches of confidentiality: under no circumstances should students be allowed to use the staff laptops/devices if not directly supervised by a member of staff. Staff should also be cautious when using the computer away from school particularly with files which may contain personal student data.

8. The laptop/device will be recalled from time to time for maintenance / upgrade and monitoring.

I have read and agree to the terms and conditions in this agreement.
I undertake to take due care of the computer and return it when requested.

Signed:_____

Date:_____

This policy should be read in conjunction with the school's Safeguarding Policy and Procedures (including Child Protection). All our practice and activities must be consistent and in line with the Safeguarding Policy and Procedures noted above. Any deviations from these policies and procedures should be brought to the attention of the Headteacher so that the matter can be addressed.