IT Acceptable Use Policy (Students)

1. Introduction

1.1 Eastern High provides computing hardware and software (including device native and cloud-based software and services) to enable all user groups the access to meet their needs.

1.2 This policy aims to ensure that the integrity of the school network and systems is upheld, and that these facilities are always available.

1.3 To ensure that each student understands and agrees to the content of this policy, it is incorporated into the home school agreement signed by students and parents.

2 Scope

2.1 This policy applies to all students accessing information technology (IT) resources owned, operated, or provided by Eastern High.

2.2 Students includes all Eastern High students and visiting students.

2.3 All information transmitted or stored on school IT resources is the property of the school unless it is specifically identified as the property of other parties.

2.4 The terms and conditions listed in the acceptable usage policy are not exhaustive as the use of technology is constantly developing. However, the policy does aim to cover all usage that is commonplace with the school.

3 Security

3.1 Student are responsible for the security of their account(s) and files and must:

✓ Take full responsibility for the security of any device that is assigned to them for work in or outside of school.

✓ Adhere to any additional security measures implemented or changed by the school, such as multifactor authentication. This includes ensuring personalised accounts use the optimal security methods that are offered by a service or software provider.

✓ Ensure their username and passwords are not passed on to anyone else.

✓ Passwords must be complex; a minimum of 10 characters, which must include uppercase and lowercase letters, numbers and special characters.

Students must not:

X Allow anyone else to access their account(s).

X Use another persons' account to login to any school systems or service

X Attempt to gain access to unauthorised areas of the school network.

X Attempt to interfere with the school network or IT equipment.

X Attempt to download, store or install software to school computers.

X Attempt to introduce a virus or malicious code to the network.

X Attempt to bypass network or system security.

X Attempt to use any form of hacking/cracking software or system.

x Connect USB devices to school devices

X Connect any device to the network that acts as a Wireless Access Point (WAP), bridge or router.

X Connect any device to the network that has access to the Internet via a connection not provided by the school.

X Access, download, create, store or transmit material that is indecent or obscene, could cause annoyance or offence or anxiety to others, infringes copyright or is unlawful, brings the name of the school into disrepute.

X Take images or videos of individuals within the school, without their permission.

X Engage in activities that waste technical support time and resources.

4 Use of Software and Services:

4.1 The software required for students will be decided and supplied subject to approval by Eastern High.

4.2 Under no circumstances should students download or install any software, (this includes apps, games, screen savers etc) unless authorised by the IT team.

4.3 The IT team carry out automated checks of the school network, if any unauthorised software is found, it will be deleted and reported.

5 Portable Devices

5.1 All portable devices and accessories remain the property of the school and should not be removed from school premises unless a loan has been agreed.

5.2 Personal data should only be stored on a portable device when it is essential to do so, and it has been encrypted and held under the guidance of the General Data Protection Regulation 2018.

5.3 Software should not be installed onto the portable devices unless it has been authorised and provided by a member of the school's IT Support team.

5.4 Portable devices will not be allowed to connect to the school network.

6 Use of own devices

6.1 Any mains-operated personal computer or electrical equipment brought on site, for any use, is subject to a Portable Appliance Test (PAT) by qualified staff and must not be used until approved. This test must be performed at regular intervals within a 3-year cycle.

6.2 Students must not connect personal computer equipment to school IT equipment without prior approval from the IT Staff.

6.3 Personal devices should never be used for taking any images or videos of individuals within the school.

7 School Email Use

7.1 Students using the school network are responsible for the content of all text, audio, images, and files that they send from or to the school email system.

7.2 School email should not be considered private as it may be accessed by IT technicians under certain circumstances.

7.3 The school's email system must not be used for the transmission, retrieval or storage of any messages which are harassing, defamatory, obscene, offensive or breach copyright regulations. Any such emails received should be reported immediately.

7.4 If a user receives an email from an unknown person or that is offensive or upsetting, the relevant house support officer or a member of the IT department should be contacted. Do not delete the email in question until the matter has been investigated.

7.5 Do not open attachments from senders you do not recognise, or that look suspicious.

8 Access to Email

8.1 Access to and usage of email must be in accordance with this policy

8.2 Email access is provided to all devices connected to the school network. The school reserves the right to withdraw access to internal or external email from any device, or any individual, at the discretion of the school if misuse is evident or suspected.

8.3 Students are not allowed to use email during lessons, unless the teacher for that lesson has permitted its use.

9 Use of Social Networking Services and Online Forums

9.1 The use of Instant Messaging (IM), and some social networking (SN) sites is allowed. Social media sites generally have an age restriction of 13. Age restrictions must be adhered to.

9.2 Students are not allowed to use IM/SN facilities during lessons unless the teacher for that lesson has permitted its use.

9.3 Do not use a screenname that is offensive or gives away additional personal information.

9.4 Students must take care when using social media services such as Facebook, even when such use occurs in their own time using their own computers. Social networking sites invite users to participate in formal ways that can leave individuals open to abuse.

9.5 Students should protect their personal information and ensure it is not accessible via a 'Public' setting. Where Possible set social media accounts to a 'Friends only' level of visibility.

9.6 Students should take steps to ensure that any person making contact via a social network service is who they claim they are, and not an imposter, before allowing them access to personal information.

9.7 Students should also take care when posting to any public website (including any online discussion forums, or blogs) that their comments do not harm their professional standing or the reputation of the school, even if their online activities are entirely unrelated to the school.

9.8 Unless authorised to do so, users must not post content on social media or websites that is presented to be, or may appear to be, on behalf of the school.

9.9 Students must not post any material online that can be clearly linked to the school or that may damage the school reputation.

9.10 The use of video and voice facilities within IM/SN is not permitted unless being supervised by a teacher.

9.11 Do not add or allow your profile, screen-name or contact information to be shown in online public directories.

10 School Internet and Wi-Fi Services

10.1 All internet traffic on the school network is monitored, logged and is subject to the implementation or change of restrictions to websites and services.

10.2 Under no circumstances should students download, use, or upload any material likely to be unsuitable, not directly related to school business or liable to offend others. This applies to any material of a violent, dangerous, racist, extremist, or sexual nature.

10.3 The school has Internet Monitoring and Safeguarding tools in place and under no circumstances should students attempt to circumvent this. Impero is installed on all school owned devices and is used for monitoring any misuse. The software tracks and monitors all user activity on school devices.

10.4 Users should not copy and use material from the Internet to gain unfair advantage in their studies, for example in coursework. Such actions may lead to disqualification by examination boards.

11 Reporting Incidents

Students of Eastern High have a responsibility to:

11.1 Inform the IT team or teacher immediately of any abuse of the IT systems, software, or hardware.

11.2 Inform the IT team or teacher immediately of any inappropriate content or misuse or if this is suspected on any of the schools IT systems

11.3 Inform the IT team immediately of actions by others if they are in breach of this policy.

12 Confidentiality and Copyright

12.1 All Students must respect the work and ownership rights of people outside the school.

12.2 Each individual user is responsible for complying with copyright law and licences that may apply to software, files, graphics, documents, messages, and other material you wish to use, download or copy. Even if materials on the school computer system or the Internet are not marked with the copyright symbol (©), it should be assumed that they are protected under copyright laws unless there is an explicit permission on the materials to use them.

12.3 By storing or creating any personal documents or files on the school computer system, users grant the school a non-exclusive, universal, perpetual, irrevocable, and royalty-free licence to use, copy, and distribute those documents or files in any way the school sees fit.

13 Action in the event of a Policy breach

13.1 Any accidental breach of this policy should be reported to the Information & Communications Manager immediately.

13.2 Any student who deliberately or carelessly breaches the rules of this policy may be investigated under the school's disciplinary procedures and this could lead to exclusion.

13.3 Any student who deliberately or carelessly breaches the rules of this policy will be reported to IT Support and their access to school resources could be removed immediately.

14 Support

14.1 If you have any questions, comments or requests with regards to the systems in place, please do not hesitate to contact a member of the IT department

14.2 Faulty equipment should be reported to the IT services department in person or by sending an email to itservices@easternhigh.org.uk. Users should not attempt to repair equipment themselves.