THE ELTON HIGH SCHOOL

ONLINE SAFETY POLICY

Date Prepared	February 2019
Date agreed by Governors	11 March 2019
Date to be reviewed	February 2021
Person responsible	Daley Thompson

This document outlines The Elton High School's policy to ensure safe access for students, staff, parents, governors and others who may access the school's computers, network services and Internet.

Benefits

Internet access is planned to enrich and extend learning opportunities across the curriculum. The Internet, Virtual Learning Environment (VLE) and e-mail enables staff and students to:

- explore libraries, museums and education sites;
- communicate with others in the local community and the wider world;
- publish and display work on the school website.

Safety

All Internet access is logged so that Web activity can be monitored. To ensure the safety of everyone in our community, the school will:

- always use an Internet Service Provider that filters access to sites and pages on Internet;
- always supervise students use of the Internet;
- ensure photographs or pictures are of a general group or class nature;
- ensure individuals are not named on web pages and that labels are of a general nature e.g. Geography by Year 8;
- make all parents or guardians of students aware of the contents of this policy.

Student Guidelines

Students will be educated in responsible and effective Internet use. Students will:

- only use the Internet with permission and when a teacher or approved adult is present;
- not give out passwords or personal details, including last name, about themselves or others;
- only to use the Internet in connection with their studies;
- learn to copy, save and use material found on the Internet without infringing copyright;

- not attempt to access any site or information that may be deemed unsuitable;
- not send, display or store offensive messages pictures or other materials;
- not use or send obscene, insulting or racist comments which might harass others;
- not use, access or amend the folders, work or files of other users.

Staff and Adult Guidelines

Staff and other adults must act responsibly when using computers and the Internet. All staff agree to the below Acceptable Use Policy. A copy is signed by each member of staff and is available on the desktop each time they log onto the school's system.

The Elton High School-Staff ICT Acceptable Use Agreement/Code of Conduct

ICT and related technologies (such as email, the internet and mobile devices) are an expected part of our daily working life in school. This policy is designed to ensure that all staff are aware of their professional responsibilities when using any form of ICT. All staff are expected to sign this policy and adhere to at all times to its contents. Any points of clarification should be discussed with the Headteacher.

Members of Staff:

- Should only use the school's email/Internet/Intranet/Learning Platform and any related technologies for professional purposes.
- Will make reasonable personal use of some ICT resources. 'Reasonable personal use' means private use that is infrequent, brief and kept to a minimum. It is reasonable provided it is not **prohibited use** as defined by this policy.
- Must support and promote the school's Online Safety policy and help students to be safe and responsible in their use of ICT and related technologies. Staff will report issues of bullying or racial hatred straight away to the school designated safeguarding officer.
- Must not browse, download, upload or distribute any material that could be considered offensive, illegal or discriminatory. Such actions may result in criminal proceedings
- Must only use the approved, secure email system(s) for any school business.
- Must ensure that when accessing email and CPOMS outside of school that they completely log out of their account when finished.
- Must ensure that all electronic communications with students and staff are compatible with their professional role.
- Must understand that email or text communication with a child outside of agreed protocols, may lead to disciplinary and/or criminal investigations.
- Must ensure images and personal information of students and/or staff will only be taken, stored and used for professional purposes in line with the school's Photographic Images Policy and Data Protection Policy.
- Should only use school provided equipment for taking photographs of students. Images will be downloaded to the school server.
- Should not use their own equipment to take images of students. Seek permission from the safeguarding officer/Headteacher to use personal equipment. Download any material direct to school equipment.
- Should respect copyright and intellectual property rights e.g not storing videos/images/information on school network that might be a copyright infringement issue.
- Must ensure that they do not use their own mobile phone to communicate with students/parents, unless dialling 141 or withholding your own personal number. Wherever possible, ensure school phones are used. A school mobile is available from the business manager for school trips.
- Must not encourage students to socialise with staff on gaming sites. The use of online gaming websites in school is prohibited.

- Have a duty to comply with the ICT system security and not disclose any passwords provided to them by the school or other related authorities.
- Should ensure that personal data (such as data held on SIMS) is kept secure and is used appropriately, whether in school, taken off the school premises or accessed remotely. Files held on USB devices must be encrypted, or the device must be encrypted.
- Will only share personal information with third party online service suppliers with the Data Protection Officer's authority.
- Should ensure that their use of web 2 technologies, including social networking sites, such as Facebook, Twitter, YouTube, does not question or bring their professional role into disrepute. Members of staff:
    - Are advised to consider, and set appropriately, their privacy settings on such sites. Check these settings regularly.
    - Should consider the appropriateness of images and material posted. Once posted online, a message, photo or video clip can be freely copied, manipulated and circulated and will potentially exist forever.
    - Should not communicate with students, in relation to either school or non school business, via web 2 technologies. Members of staff should only communicate with students using the appropriate LA/school learning platforms or other systems approved by the Headteacher.
    - Do not accept students/parents as friends on social media accounts.
    - Do not accept students that leave the school as friends. This could allow other students access to your profile.
    - Be aware that belonging to a 'group' can be a 'back door' into your profile.
- Must not install any hardware or software without permission of the ICT Co-ordinator/Headteacher.
- Must not connect a computer or laptop to the network/internet that does not have up to date anti-virus software.
- Understand that all use of the internet and other related technologies can be monitored and logged and can be made available by request, to the Headteacher or governing body.
- Have a responsibility to report any misuses of technology, including the unacceptable conduct of others, to the Online Safety coordinator or Headteacher.

User Signature

I agree to follow this code of conduct and to support the safe use of ICT throughout the school.

Signature……

Full Name…… (printed)

Job Title ……

Email

Every student at The Elton High School has an e-mail address. All e-mails containing banned phrases are blocked by the schools e-mail filter. Students should only e-mail for work related matters, not a messaging service. Anyone found using Chat Rooms and instant messaging inappropriately will lose their account. Students will be made aware of the dangers of using these.

Blogs and Wikis

As this develops as a teaching tool, care will be taken to:

- ensure that those used for teaching and learning are safe
- all students and staff are aware of the security issues involved with using these.

The school has its own website www.eltonhigh.bury.sch.uk

The website is used to:

- promote the school and community;
- post important dates
- celebrate success via The Elton Times, the schools newsletter
- link to appropriate websites to support the curriculum

Procedures

The Assistant Headteacher (designated Online Safety Coordinator) and/or Headteacher may at any time, without prior notice:

- check personal files and computers hard disk drives for viruses or unsuitable material;
- review lists of Internet sites logged on computers for inappropriate use of the Internet;
- check e-mail for viruses or unsuitable material.

Sanctions

Sanctions will be enforced on violations of the Agreed Acceptable Use of Computers and the Internet Policy. These may include:

- temporary or permanent bans from using the Internet and/or e-mail;

- sanctions for students in line with those agreed in the current Behaviour Policy Document;
- sanctions for adults in line with those set out in conditions of employment documents;
- prosecution by the police. The possession of certain types of unsuitable materials is a criminal offence
- civil prosecution for libel and defamation.

Related Issues

The Elton High School is appropriately registered under the Data Protection Act:

- to hold information about individuals such as students and staff on computers;
- for Internet use, including emails;
- to publish information on a school website.

All information held about individuals such as students or staff on computers is password protected. Access to computers on which such information is held is restricted.

Promoting Online Safety

The following steps are taken to promote Online Safety at The Elton High School:

- Useful websites, such as www.thinkyouknow.co.uk;
- All students are taught about online safety in ICT/Computing lessons and are aware of the CEOPS button;
- Online safety assemblies for all students held annually;
- Online safety is an integral part of the Computing curriculum and is also covered though the Student Development Day programme.

Hand held devices

Hand held devices, Mobile phones and, in particular, the new generation of smart phones, such as the iPhone, now include many additional functions such as an integrated camera, video recording capability, instant messaging, mobile office applications and mobile access to the internet. These allow immediate access to email, searching for information on the internet and other functions such as access to social networking sites e.g. Facebook, twitter and blogging sites.

For many young people today the ownership of a mobile phone is considered a necessary and vital part of their social life. When used creatively and responsibly the smart phone has great potential to support a student's learning experiences.

Bullying, intimidation and harassment are not new in society; however bullying using a mobile phone represents a new challenge for schools to manage.

Parents and students should be clear that misuse of mobile phones will not be tolerated. The following are examples of misuse but are not exclusive:

- the deliberate engineering of situations where people's reactions are filmed or photographed in order to humiliate, embarrass and intimidate by publishing to a wider audience including social media platforms
- bullying by text, image, instant and email messaging
- the use of a mobile phone for 'sexting' (the deliberate taking and sending of provocative images or text messages)
- students posting material on social network sites with no thought to the risks to their personal reputation and sometimes with the deliberate intention of causing harm
- making disrespectful comments, misrepresenting events or making defamatory remarks about teachers or other students
- general disruption to learning caused by students accessing phones in lessons
- students phoning parents immediately following an incident so that the ability of staff to deal with an incident is compromised
- publishing photographs of vulnerable students, who may be on a child protection plan, where this may put them at additional risk.

Dealing with breaches

Misuse of the mobile phone will be dealt with using the same principles set out in the school behaviour policy, with the response being proportionate to the severity of the misuse.

Students are aware that serious misuse may lead to the confiscation of their mobile phone, communication with parents and the imposition of other sanctions up to and including exclusion from school. If the offence is serious it will be reported to the Police.

When a mobile phone is confiscated, the confiscation procedure will be followed to ensure that the confiscation is correctly recorded and that the phone is kept securely.

Where it is deemed necessary to examine the contents of a mobile phone this will be done by a designated member of staff.

The action will be properly recorded in case it later becomes evidence of criminal activity. The record will include the time, who was present and what was found.

Rules for the Acceptable Use of a mobile phone in school by students

Students are allowed to bring a mobile phone into school. If they choose to do so it is on the understanding that they agree with the following limitations on its use, namely:

- The phone must be kept out of sight and turned off,
- Mobile phones must be switched off at all times during the school day, including break and lunchtimes, and remain off whilst students are on the school premises. It is not acceptable for phones merely to be put on silent or pager mode
- Mobile phones can be used in the classroom with the agreement and under the direction of staff eg access to revision sites, research or quizzes.
- No student may take a mobile phone into a room or other area where examinations are taking place
- The security of the phone will remain the student's responsibility in all lessons including Physical Education lessons
- If asked to do so, content on the phone (e.g. messages, emails, pictures, videos, sound files) will be shown to a teacher

Unacceptable use

The school will consider any of the following to be unacceptable use of the mobile phone and a serious breach of the school's behaviour policy resulting in sanctions being taken.

- Photographing or filming staff or other students without their knowledge or permission
- Photographing or filming in toilets, changing rooms and similar areas
- Bullying, harassing or intimidating staff or students by the use of text, email or multimedia messaging, sending inappropriate messages or posts to social networking or blogging sites
- refusing to switch a phone off or refusing to hand over the phone at the request of a member of staff
- using the mobile phone outside school hours to intimidate or upset staff and students will be considered a breach of these guidelines in the same way as unacceptable use which takes place in school time
- using a mobile phone outside school hours in such a way that it undermines the stability of the school and compromises its ability to fulfil the stated aim of providing 'a clear moral and ethical lead'.

Sanctions

Students and parents are notified that appropriate action will be taken against those who are in breach of the acceptable use guidelines, following the schools behaviour policy.

- students and their parents should be very clear that the school is within its rights to confiscate the phone where the guidelines have been breached.

Using the mobile phone outside school hours to intimidate or upset staff and students or undermine the stability of the school in any way will be considered a breach of these guidelines in the same way as unacceptable use which takes place in school time.

- If a phone is confiscated, school will make it clear for how long this will be and the procedure to be followed for its return

- Students should be aware that the police will be informed if there is a serious misuse of the mobile phone where criminal activity is suspected
- If a student commits an act which causes serious harassment, alarm or distress to another student or member of staff the ultimate sanction may be permanent exclusion. School will consider the impact on the victim of the act in deciding the sanction.

Confiscation procedure

If a mobile phone is confiscated then:

- the student will be informed that the phone can be collected at the end of the next school day from the school reception. If confiscated on a Friday, the phone can be collected at the end of that day.
- the confiscation will be recorded in the school behaviour log for monitoring purposes
- school will ensure that confiscated equipment is stored in such a way that it is returned to the correct person
- in the case of repeated or serious misuse the phone will only be returned to a parent/carer who will be required to visit the school by appointment to collect the phone. This may be at the end of a week, a half term or longer. At the discretion of the Headteacher the phone may be returned to the student at the end of the confiscation period.
- where a student persistently breaches the expectations, following a clear warning, the Headteacher may impose an outright ban from bringing a mobile phone to school. This may be a fixed period or permanent ban.

Where the phone has been used for an unacceptable purpose

- The Headteacher or a designated staff member will have the right to view files stored in confiscated equipment and if necessary seek the cooperation of parents in deleting any files which are in clear breach of these guidelines unless they are being preserved as evidence

- If required evidence of the offence or suspected offence will be preserved, preferably by confiscation of the device and keeping it secure or by taking photographs of the screen
- School will consider whether an incident should be reported to MASH.
- The designated staff member should monitor repeat offences to see if there is any pattern in the perpetrator's or the victim's use which needs further investigation.

Looked after students (CYPiC)

There may be a safeguarding concern if a CYPiC, who has limited contact, or supervised-only contact with a parent, suddenly acquires a mobile phone as this could have been provided by the parent to maintain contact. This should be discussed with the designated teacher for CYPiC in school.

Young carers

Some young carers only feel able to attend school because their mobile phone enables easy access with the person they care for and may react strongly to a ban on phones or restrictions on their use. This will need to be treated sensitively by the school.

Child sexual exploitation (CSE).

1) A feature of some of the recent cases where teenage girls have been groomed for sex has been giving them expensive phones as a gift. The unexpected acquisition of an expensive mobile phone by girls who are unlikely to be able to afford one themselves should trigger a safeguarding concern.

2) The same approach is often used to draw children into selling drugs.

3) Where such issues/concerns are raised, staff should report to the designated safeguarding officer for further investigation.

Further Guidance

Confiscation and screening

http://www.education.gov.uk/schools/studentsupport/behaviour/f0076897/screening

Newsround article on happy slapping including advice for students on what to do if it happens to them

http://news.bbc.co.uk/cbbcnews/hi/newsid_4490000/newsid_4498700/4498719.stm

cyberbullying resource page:

http://www.childline.org.uk

Child Exploitation and Online Protection Centre

http://www.ceop.police.uk

Think U know

https://www.thinkuknow.co.uk/

Internet Watch Foundation (IWF)

https://report.iwf.org.uk/en/

Suspected online terrorist material

https://www.gov.uk/report-terrorism

Safeguarding concerns which may be raised by mobile phone use in school

Some useful sites:

https://www.gov.uk/government/collections/ofsted-inspections-of-maintained-schools

www.childnet.com

www.dangerpoint.org.uk

http://www.saferinternet.org.uk/advice-and-resources/teachers-and-professionals/esafety-policy

http://webarchive.nationalarchives.gov.uk/20130401151715/http://www.education.gov.uk/publications/eOrderingDownload/BEC1-15535.pdf

Greater Manchester Safeguarding Procedures (E-safety procedure/guidance)

http://greatermanchesterscb.proceduresonline.com/pdfs/e_safety.pdf

http://greatermanchesterscb.proceduresonline.com/chapters/contents.html

Manchester's E-safety policy

http://www.manchesterscb.org.uk/docs/esafety Minimum Standards V3.pdf

digital parenting magazines

http://www.vodafone.com/content/parents/digital-parenting/magazines.html

External Consultant and reviewer of policy:

Mark Gay

Bury Local Authority Designated Officer (LADO)

Bury Safeguarding Unit