E-Safety Guide for Staff

Weatherhead High School has appointed the e-Learning Co-ordinator as the e-Safety Co-ordinator.

This guidance is supported by our Acceptable Use Policy for staff and a separate version suitable for students; the Policy on the Use of Social Networking Websites; and the Policy on the Use of Photography/Film.

This e-safety guidance and our Acceptable Use Policies are agreed by the Board of Governors and reviewed annually. This policy will next be reviewed in July 2024.

Why is internet use important?
New technologies have become integral to the lives of children and young people in today's society, both within school and in their lives outside school. It is an essential element in 21st century life for education, business and social interaction. The internet and other digital information and communications technologies are powerful tools, which open up new opportunities for everyone. These technologies can stimulate discussion, promote creativity and stimulate awareness of context to promote effective learning. Internet use is part of the curriculum and a necessary tool for learning. It can raise educational standards, promote student achievement, support the professional work of staff and enhance the school's management information and administration systems. It also brings opportunities for staff to be more creative and productive in their work.

All users, who show a responsible and mature approach to its use, should have an entitlement to safe internet access at all times.

Students will use the internet outside school and will need to learn how to evaluate internet information and to take care of their own safety and security. Guidance on this is provided during assemblies, form time activities, ICT and PSHCE lessons and many other curriculum activities.

How does internet use benefit education?
Benefits of using the internet in education include:-

- Access to learning wherever and whenever convenient.
- Access to world-wide educational resources including museums and art galleries.
- Educational and cultural exchanges between students world-wide.
- Access to experts in many fields for students and staff.
- Professional development for staff through access to national developments, educational materials and effective curriculum practice.
- Collaboration across support services and professional associations.
- Improved access to technical support including remote management of networks and automatic system updates.
- Exchange of curriculum and administration data with the Local Authority and DfE.

How can internet use enhance learning?

- The school internet access is designed expressly for student use and includes filtering appropriate to the age of students.
- Students will be taught what internet use is acceptable and what is not and will be given clear objectives for internet use.
- Internet access will be planned to enrich and extend learning activities.
- Staff will guide students in on-line activities that will support learning outcomes planned for the students' age and maturity.

- Students will be educated in the effective use of the internet in research, including the skills of knowledge location, retrieval and evaluation.

Authorised Internet Access

- The school will maintain a current record of all staff and students who are granted internet access.
- All staff must read and sign the Acceptable Use Policy (AUP) before using any school ICT resource.
- The Acceptable Use Policy extends to the use of school devices/platforms used off site and personal devices used to access the school network or for school related activities off-site.
- Parents/carers will be informed that students will be provided with supervised internet access.
- Students must apply for internet access individually by agreeing to comply with the AUP.
- KS3/4 parents/carers and all students will be asked to sign and return a consent form for student access.
- Use of the internet and facilities such as e-mail are intended for educational purposes only. Any view communicated over the internet may be deemed to be a view of the school akin to formal correspondence issued by post. Personal views about the school in an electronic communication should not be given or must be endorsed by the Headteacher or a member of the Senior Leadership Team.

The Internet

- If staff or students discover unsuitable sites, the URL (address), time and content must be reported to the e-Learning Co-ordinator and recorded in the e-safety log.
- Wherever possible, the school will ensure that the use of internet derived materials by students and staff complies with copyright law.
- Students should be taught to be critically aware of the materials they are shown and how to validate information before accepting its accuracy. Whenever possible, staff should always check the online content they are intending to use with students in the classroom beforehand to see if the site is accessible and to check the appropriateness of the content and surrounding content.

Online Learning

- Staff and students must sign the school's AUP for access to the school's learning platforms.

Email

- The email system is for professional business purposes only, and not for any personal requests.
- Staff and students may only use approved web based e-mail accounts on the school system.
- Whenever e-mail is sent, the sender's name, job title, e-mail address and the school's name must be included.
- When sending e-mails, please be mindful of your intended audience to avoid colleagues receiving unnecessary information.
- On occasion staff may receive e-mails out of school hours. Where this occurs there is no expectation for staff to respond or action until the following working day.
- Every user is responsible for all mail originating from their user ID (e-mail address).
- Forgery or attempted forgery of electronic mail is prohibited.
- Attempts to read, delete, copy or modify the e-mail of other users are prohibited.
- Attempts to send junk mail and chain letters are prohibited.
- Staff must immediately tell a member of the SLT if they receive an offensive e-mail.
- Staff must not reveal personal details of themselves or others in e-mail communications.

- Access in school to external personal e-mail accounts may be blocked at certain times of the day.
- Only departmental e-mail addresses should be used in communications with parents and carers e.g. *businessdept@weatherheadhigh.co.uk*. Under no circumstances should staff communicate with parents/carers or students using their own personal e-mail address.

Password Protection

- The school issues passwords.
- Staff and students are encouraged to use a strong password.
- No use of generic passwords.
- Passwords must not be disclosed to staff or students.
- Staff and students are educated on what constitutes a strong password.

Social Networking

- The school blocks/filters access to social networking sites and newsgroups unless a specific use is approved and logged in the e-safety log.
- Students are advised never to give out personal details of any kind which may identify them or their location.
- Students are advised not to place personal photos on any social network space that would identify their school or where they live.
- Students are advised on security and encouraged to set passwords, deny access to unknown individuals and are instructed on how to block unwanted communications.
- Students should be encouraged to invite known friends only and deny access to others.
- Assemblies and up-to-date presentations are presented throughout the school year and with the introduction of emerging technologies.
- Staff are not to have students, parents/carers as contacts on their personal social networking profiles.
- Staff are not to converse about school related issues or students on social networking sites.
- Staff and students are to ensure they understand the platforms they use and the privacy functions within.
- Staff at Weatherhead are to adhere to the locally agreed Social Networking Policy.

Filtering & Monitoring

- The school will work in partnership with Hi-Impact to ensure filtering systems are as effective as possible.
- All student computers are monitored using Securus to help identify harmful content and misuse in online and offline applications.

Cyberbullying

- Bullying in any form will not be tolerated at Weatherhead. Cyberbullying will be dealt with in line with the school's Anti-bullying Policy.

Video Conferencing

- Students should ask permission from the supervising teacher before making or answering a video conference call.
- Video conferencing will be appropriately supervised for the students' age.

USB memory sticks and other Portable Data Storage Devices

- Staff are not to have any unprotected sensitive student data stored on USB or external hard-drive devices that go off site. If in doubt as to appropriateness, advice can be sought from the e-Learning Co-ordinator.
- Sensitive data should be encrypted; advice on how to do this can be obtained from the ICT Technicians and e-Learning Co-ordinator.

Portable Devices (e.g. laptops or tablets)

- If you have information about learners on your laptop or tablet (e.g. data or registers), you should ensure that no unauthorised person uses your device. You are responsible for ensuring password protection for the data on your device.
- The AUP applies to school equipment/software made available to you for use at home and in school.

Digital Cameras

- Staff are to only use school equipment to photograph students.
- Staff must not use personal equipment to photograph students unless permission has been granted to upload images to one of the school's social networking sites directly from personal equipment e.g. a smartphone. This will be of particular relevance to trips abroad.
- Storage cards are to be cleared when the camera is returned.

Storage of Photographs

- Photographs must be stored in a secure area within the school network on the staff shared area: S:\Admin\School Photo Archives
- Photographs are to remain on school premises when practicable. Images taken off-site, for example on a school trip, should only be downloaded onto the school network.
- Photographs are to be deleted when no longer required.
- The school's policy on 'Use of Photography/Film' must be adhered to regarding photographing and publishing images of children.

Smartphones and other Hand Held/Communication Devices

- Smartphones and other hand held communication devices should not be used for personal use in the lesson or formal school time (students and staff).
- Smartphones – Bluetooth should be turned off at all times.

Published Content, the School Website and Social Networks

- The contact details on the website will be the school address, e-mail and telephone number. Staff or students' personal information will not be published.
- A designated member of the SLT, assigned by the Headteacher, will take overall editorial responsibility and ensure that content is accurate and appropriate.

Guidelines for Using Departmental Social Media Accounts

- Social media platforms are a public space and school accounts should be used in line with the school's e-safety guidance and Acceptable Use Policy.
- Social media accounts should be approved by the department SLT Mentor prior to activation. Please inform the e-Learning Co-ordinator so accounts can be monitored and promoted.
- Accounts should be linked to a departmental email address, e.g. *businessdept@weatherheadhigh.co.uk* and the password known to key members of departmental staff.
- Use a strong password; keep passwords secure.
- Curriculum accounts should be used to follow industry experts, professional bodies and educators; this may include the professional accounts of Weatherhead staff and curriculum accounts.
- Professional language should be applied at all times; avoid slang/text style language.
- Do not follow student accounts or the personal accounts of Weatherhead staff.
- Encourage students to *'protect'* their accounts using the platform's privacy settings.

- Do not send private/direct messages (DM) to students.
- Check hashtags before including them in posts; some hashtags may bring up inappropriate results as part of the search.
- Accounts must be monitored regularly by the Curriculum Leader or Head of Department; curriculum accounts will be monitored by the e-Learning Co-ordinator.
- Please be aware that not all students will have regular access to the internet; important messages and notices must be available in an alternative location for those students and be issued with enough advanced notice.

Publishing Students' Images and Work

- The school's policy on 'Use of Photography/Film' must be adhered to regarding photographing and publishing images of children.
- Photographs that include students will be selected carefully and will be appropriate for the context.
- Students' full names will not be used anywhere on the website, VLE or the school's Social Networks, particularly in association with photographs.
- Students listed on the Photo Non-Consent list MUST NOT be used in any digital or printed publication unless permission has been sought from the parent or guardian. Always refer to the current Photo Non-Consent located on the staff shared area: S:\Admin\Photo Consent

Information System Security

- School ICT systems' capacity and security will be reviewed regularly.
- Virus protection will be installed and updated regularly.
- See also 'USB memory sticks and other Portable Data Storage Devices'.

Cyber Crime and Cyber Security

Cyber crime may involve malicious attacks on computer software, including:

Email hacking

Email hackers try to gain access to email accounts by tricking people:

- to open and respond to spam emails
- to open emails with a virus
- to open phishing emails

Phishing

Phishing messages look authentic with corporate logos and a similar format to official emails. Unlike official communications, phishing email ask for verification of personal information such as account numbers, passwords or date of birth. Unsuspecting victims who respond may suffer stolen accounts, financial loss and identity theft.

Malvertising

Malvertising can compromise computers by downloading malicious code when people hover on or click on what looks like an advert. Some will even download malicious code to your computer, while the website is still loading in the background. Cybercriminals use advertisements as a way to hack into computers.

Ransomware

Ransomware is malicious software which could be delivered to devices in a number of ways. One of the common ways is via emails and email attachments. This malicious software is designed to deny access to your systems / records and charge a fee to reinstate access, or sometimes the intent may simply be to gain unauthorised access to data you hold.

Denial of Service Attacks
Denial-of-service attacks are a cyber-attack in which the perpetrator seeks to make a machine or network unavailable. The majority of the time this is simply to cause a nuisance, but on other occasions it may be used to disguise a network intrusion and compromise of data.

Staff **MUST** ensure that they:

- check the sender of an email is genuine before, for example, sending payment, data or passwords or opening an attachment.
- make direct contact with the sender (without using the reply function) where the email requests a payment.
- understands the risks of using public wifi.
- understand the risks of not following payment checks and measures.
- never enter or share personal information e.g. account details, passwords.
- remain vigilant.

This is not an exhaustive list.

Protecting Personal Data
Personal data will be recorded, processed, transferred and made available according to the General Data Protection Regulations 2018.

Assessing Risks
The school will take all reasonable precautions to prevent access to inappropriate material. However, due to the international scale and nature of linked internet content, it is not possible to guarantee that unsuitable material will never appear on a school computer. The school cannot accept liability for the material accessed, or any consequences of internet access.

The school will audit ICT use to establish if the e-safety policy is adequate and that the implementation of the e-safety policy is appropriate every 12 months.

Appendices: Acceptable Use Policy
Policy on the Use of social Networking Websites
Use of Photography/Film