E-Safety Policy

Governance Status

This policy was created in June 2014 and was adopted by the Governing Body on 16 June 2014. It will be renewed every two years or in the light of new guidance or legislation.

Review dates	By Whom	Approval dates
January 2020	Staff and Governors	24 March 2020
March 2023	Staff and Governors	11 July 2023
May 2025	Staff and Governors	20 May 2025

Signed by the Chair of Governors:

E-Safety Policy

Contents

1. Introduction

Whitby School is a KS3/4 school catering for the educational needs of its pupils and preparing them for life after their tenure. The schools are extremely progressive in their approach to technology, to inform, educate and to facilitate learning to all users by utilising the best possible ICT equipment. This increasing development of ICT for curricular and administrative purposes is allowing pupils and staff to access a wider range of information more effectively and develop capabilities in the wide range of possibilities ICT can offer. This may be a student conducting research on the Internet, a member of administrative staff mail-merging letters from a database, members of the community accessing open-learning resources or a teacher analysing student performance, or parents accessing their child's record through the Virtual Learning Environments.

2. Policy Statement

Whitby School recognises the benefits and opportunities which new technologies offer to teaching and learning. We provide internet access to all learners and staff and encourage the use of technologies in order to enhance skills, promote achievement and enable lifelong learning. However, the accessibility and global nature of the internet and different technologies available mean that we are also aware of potential risks and challenges associated with such use. Our approach is to implement appropriate safeguards within the schools, while supporting staff and learners to identify and manage risks independently and with confidence. We believe this can be achieved through a combination of security measures, training such as CEOP, guidance and implementation of our policies. Unfortunately, the likelihood of breaches of system integrity increases with the more frequent access to the network and the programmes contained therein. To safeguard learners, we will do all that we can to make our learners and staff E-safe and to satisfy our wider duty of care. This E-safety policy should be read alongside other relevant policies and legislation.

3. Policy Scope

This policy applies to all users (staff, pupils and visitors) who have access to the schools' ICT systems and facilities, both on the premises and remotely. Any user of the schools' ICT systems must adhere to and sign a hard copy of the E-Safety Policy. The E-Safety Policy applies to all use of the internet and forms of electronic communication such as email, mobile phones, social media sites which are connected in any way to the schools.

4. Policy Review

The impact of the policy will be monitored regularly with a full review being carried out at least once a year. The policy will be reconsidered where particular concerns are raised or where an E-safety incident has been recorded.

5. Roles and Responsibilities

All staff are responsible for ensuring the safety of learners and should report any concerns immediately to their line manager. When informed about an E-safety incident, staff members must take particular care to emphasise that although confidentiality will be maintained it will be passed to the relevant member of staff, as a matter of priority.

Designated Safeguarding Lead

There are clear lines of responsibility for E-safety within the College. The first point of contact is the **Designated Safeguarding Lead** responsible for Child Protection and Safeguarding. They will decide the most appropriate course of action to take and which department or agency should be involved (eg, if it is a case of cyber-bullying then the Network Manager may be required to collate evidence).

All learners must know what to do and who to contact if they have any E-safety concerns. In most cases, this will be a member of staff. A confidential email address has also been set up to report incidences of bullying. Should any incident occur that relates to E-safety, this will be investigated and the evidence will be collected; relevant external agencies (eg, NYP) will be informed as necessary.

E-Safety Officer

The E Safety Officer is responsible for the implementation of policies designed to encourage a positive approach to E Safety. The designated officer responsible for E-Safety is Mr Andrew Whelan. To assist him the Network Manager and ICT team are responsible for keeping up to date with new technologies and their use, as well as attending relevant training. They will be expected to be at the forefront of any matters pertaining to E-Safety, review and update the E-Safety Policy, deliver staff training, record incidents, report any developments and incidents to the Officer responsible for Child Protection at the schools. Nominated ICT personnel are to liaise with the Local Authority and external agencies to promote E-safety within the school communities. They may also be required to deliver workshops for parents.

Pupils

pupils are responsible for using the schools' ICT systems and mobile devices in accordance with the guidelines set out in student planners, which are signed at the time of registration by pupils and parents. pupils are expected to act safely and responsibly at all times when using the internet

and/or mobile technologies. They are responsible for attending E-safety lessons as part of the curriculum and are expected to know and adhere to other relevant policies, eg, those regarding the use of mobile phones, images, cyber-bullying, etc. They must follow the reporting procedures where they are worried or concerned, or where they believe an E-safety incident has taken place involving him/her or another member of the school community.

Sanctions

Violation of the above rules will result in a temporary or permanent ban on unsupervised use of the school's computers. Violation of the above rules will result in a temporary or permanent ban on Internet access on the school's network. Violation of the rules outlined in 'pupils access to the internet' will result in a temporary or permanent ban on Internet access on the school's network. Additional disciplinary action may be added in the line with existing practice depending upon severity of misuse. When applicable, police or local authorities may be involved.

Age appropriate information should be given every academic year to every pupil.

Staff

All staff are responsible for using schools' ICT systems and mobile devices in accordance with the computing policies, which they must sign and records will be kept by an appropriate school Officer in this respect. Staff are responsible for attending training on E-safety and displaying a model example to learners at all times through embedded good practice. All digital communications with learners must be professional at all times and be carried out in line with the Acceptable Use Agreement – ICT and E-Technology Policy. Online communications with learners are restricted to the schools' network and Twitter accounts. External platforms, not hosted by the schools, such as social media sites, should not be used to communicate directly with pupils. Any incident that is reported to or discovered by a staff member must be reported to the designated officer responsible for E-Safety and/or their line manager, without delay.

6. Security

The school will do all that they can to make sure that all users of its systems are protected by keeping the schools' network safe and secure. Data is shared to external sites to facilitate Google Classroom and other systems for the management of classroom data, e mail etc. This is in accordance with current Data Protection legislation. Every effort will be made to keep security software up to date. Appropriate security measures will include the use of web-filtering and protection by firewalls. Physical protection of data held on servers and workstations to prevent accidental or malicious access of the schools' systems and information will include access controls to hardware (such as password protection and encryption of drives as required). Data held on servers will be restricted by access permissions so that only relevant parties have access. This will be controlled by the ICT department. All staff are expected to have their USB drives encrypted either through hardware (or as hardware encryption is cost prohibitive), or software encryption programs (Bit-locker is available on all computers). Digital communications, including email and internet postings, using the schools' networks, will be monitored in line with the email and social media policies. Staff should ensure their user areas, data and emails are not left available for unauthorised access by securing/locking their machines when unattended. Data copied to personal devices (eg, emails on mobile telephones) must not be made available to unauthorised users and these devices must be secured with security unlock codes. By staff signing this policy or pupils and their parents signing the student log books / planners users are accepting that the schools' ICT departments will routinely monitor users' internet and ICT usage using school facilities.

7. Behaviour

Whitby School will ensure that all users of technologies adhere to the standard of behaviour as set out in the Staff Computing, Acceptable Use, Email and Internet Policies and any other relevant

policies). The student rules for the use of ICT and related facilities is set out in student planners. The schools will not tolerate abuse of ICT systems. Whether offline or online, communications by staff and pupils should be courteous and respectful at all times. Any reported incident of bullying or harassment or other unacceptable conduct will be treated seriously and in line with the student and staff disciplinary codes and policies.. Where conduct is found to be unacceptable, the schools will deal with the matter in accordance with agreed disciplinary procedures. Where conduct is considered illegal, the schools will report the matter to the police.

8. Communications

Whitby School requires all users of ICT to adhere to the relevant policies or in the student rules for the use of ICT and related facilities in student planners, for communications between staff and pupils. Emails from pupils to individual staff members should normally use the generic school email address with a clear identifier for the staff member concerned. Staff should normally only use the College email address for pupils through approved email groups involving other staff or by using the VLE where there is transparency and monitoring by the system administrators. For school Twitter accounts, staff are not to enter into individual dialogue or non-curriculum discussions with pupils.

9. Use of Images and Video

The use of images, or photographs, is popular in teaching and learning and should be encouraged where there is no breach of copyright or other rights of another person (eg, images rights or rights associated with personal data). This will include images downloaded from the internet and those belonging to staff or pupils.

All pupils and staff should receive training on the risks when taking, downloading and posting images online and making them available to others. There are particular risks where personal images of themselves or others are posted onto social networking sites, for example. Images or videos that are downloaded or uploaded on the schools' ICT equipment, whether for personal use or as part of learning, should not be offensive, pornographic, inflammatory or in any way bring the schools into disrepute. Images or videos of staff or pupils should not be used without consent and student images should not normally identify the student, unless parental permission is sought. Photographs of activities on the schools' premises should be considered carefully and have the consent of the headteacher, and the parties involved, before being published. Any images of pupils taken on private devices for official purposes only should be deleted as soon as they are uploaded to the appropriate school network.

10. Personal Information

Any processing of personal information needs to be done in compliance with the Data Protection Act 2018. This is likely to include content such as student records, e-portfolios and assessed work. Whitby School is legally obliged to take steps to minimise the risk that data will be lost and processed unfairly.

Personal identifiable information is information about a particular living person that can identify them to the reader. Whitby School collects and stores the personal information of pupils and staff regularly to conduct its business (eg, names, dates of birth, email addresses, assessed materials and so on). The schools will keep this information safe and secure and will not share it without the express permission of the parent/carer, unless appropriate external organisations, eg, the Local Authority or police require this for specific, legitimate purposes; this will be with the permission of the headteacher.

No personal information should be posted on the schools' websites without the permission of the headteacher. Only names and work email addresses of (senior) staff should appear on the school websites. Staff must keep learners' personal information safe and secure at all times. When using an online platform, all personal information must be password protected. Staff should have clear and definable reasons for having any personal data off-site and the permission of the headteacher. Every user of school ICT facilities is expected to log off or secure their PC or laptop on completion of an activity, or where they intend to be physically absent from a device for any period. All school mobile devices such as laptops, chrome-books, tablets and mobile telephones are required to be password protected, USB drives are to be encrypted either by built in hardware or encryption software (Bit-Locker) before leaving the premises. Where the personal data is no longer required, it should be securely deleted.

11. Education and Training

With the current unlimited nature of internet access, it is impossible for Whitby School to eliminate all risks for staff and pupils. It is our view therefore, that the schools should support staff and pupils stay E-safe through regular training and education. This will provide individuals with appropriate skills to be able to identify risks independently and manage them effectively.

For staff

Staff will take part in mandatory E-safety training at the start of the new school year through CPD sessions. This will be led by the designated person for E-safety and undertaken by relevant staff. This will normally take the format of workshops, allowing teachers hands-on experience. Further resources of useful guidance and information will be made available to staff through regular bulletins. Each member of staff must sign to indicate they have received the training and these records will be retained in school. Any new or temporary staff will receive training on the schools' ICT system, provided by ICT department staff. They will also be asked to sign the (staff) Acceptable Use Policy and E-Safety Rules.

12. Incidents and Responses

Where an E-safety incident is reported to the school, this matter will be dealt with very seriously and with urgency. Whitby School will act immediately to prevent, as far as reasonably possible, any harm or further harm occurring. If a student wishes to report an incident, they can do so to their form tutor, or via an email to an appropriate member of staff. Where a member of staff wishes to report an incident, they should contact their line manager or the member of staff designated responsible for E-safety, as soon as possible. Following any incident, the school will review what has happened and decide on the most appropriate and proportionate course of action. Sanctions may be put in place, external agencies may be involved or the matter may be resolved internally depending on the seriousness of the incident. This is in line with the Acceptable Use Policy. Serious incidents will be dealt with by senior management, in consultation with appropriate external agencies.

13. Feedback and Further Information

Whitby School welcomes constructive feedback on this and any other policy. If you would like further information on E-safety, or wish to send us your comments on our E-Safety Policy, please contact post@whitbyschool.co.uk

Whitby School E-Safety Policy User Agreement

To: The Headteacher

Name: …… (Member of staff)

I have read the 'Whitby School E-Safety Policy' and agree to its contents.

Signature: ..... (Member of staff) Date: ……