Online Safety Policy

Objective

The overall objective of this policy is to provide a safe and secure technological environment at VEC, whereby students can benefit from effective use of modern online resources, whilst being protected as far as possible from its risks.

In addition, through Online safety education and awareness, students will be equipped to protect themselves in the more open online environment that they are likely to encounter at home and in later life.

Scope and Practice

Online safety encompasses internet technologies and electronic communications such as mobile phones as well as collaboration tools and personal publishing.

Online safety depends on effective practice at a number of levels:

- responsible ICT use by all staff and students made explicit through published policies.
- sound implementation of e-safety policy in both administration and curriculum, including secure school network design and use.
- safe and secure broadband supported by appropriate filtering services.
- training and education for both staff and students.

Why is Internet Use Important?

Internet usage is ubiquitous in 21st century life, and students need to understand both its power and risks.

The purpose of internet use in school is to raise educational standards, to promote student achievement, to support the professional work of staff and to enhance the school's management information and administration systems.

Internet use is part of the statutory curriculum and a necessary tool for learning. It is an essential element in 21st century life for education, business and social interaction. Access to the internet is therefore an entitlement for students who show a responsible and mature approach to its use. VEC has a duty to provide students with quality internet access.

Non-residential 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.

For residential students, this is their home, and it is important that students are able to participate in their online life, as do their peers living at home. This includes appropriate access to social media, with appropriate safeguarding measures in place.

Risks

The following list is not exhaustive, but illustrates some of the risks that this policy is designed to protect against:

Content

- exposure to inappropriate content including online pornography
- harmful lifestyle websites, for example pro-anorexia/self-harm/suicide/substance abuse sites
- hate sites
- inaccurate and misleading content

Contact

- grooming
- sexting
- cyber-bullying in all forms
- identity theft (including social media profiles)
- Extortion

Conduct

- privacy issues, including disclosure of personal information
- digital footprint and online reputation
- health and well-being (amount of time spent online)
- copyright abuse including inappropriate use of peer-to-peer networks

Security and Content Filtering

VEC shall provide an effective filtering system that will enable appropriate access for staff and students in accordance with this policy. However, staff and students must be made aware that no filtering system is perfect, and that they may inadvertently come into contact with inappropriate content.

If staff or students discover unsuitable sites, the URL, time and content must be reported to ICS, who will arrange for filtering updates if appropriate.

Anti-virus protection and other security measures as required will be installed and updated regularly in accordance with Livability ICS policy.

Roles and Responsibilities

All members of staff are responsible for ensuring the safety of students and should report any concerns immediately to a Designated Safeguarding Officer.

At least one member of staff from Education shall have formal Online Safety training leading to an accredited Online Safety award. These staff shall take the lead in Online Safety matters and shall be available to other staff for advice and support as required.

The IT Manager is responsible for providing a secure IT environment in compliance with this policy. This includes effective filtering, and other technical measures such as the provision of 'panic buttons' to enable students to reports abuse or concerns.

All members of staff are responsible for using IT systems and mobile devices in accordance with the Acceptable Use Policy.

All digital communications between staff and students must be professional at all times. Online communication with students is restricted to VEC's network. External platforms, such as social media sites, must never be used by members of staff to communicate with students.

Online Safety Incidents

Where an Online Safety incident is reported, a CPOMS online incident form shall be submitted, and appropriate action taken through the management chain. Where appropriate, the incident shall immediately be reported to a Designated Safeguarding Officer and Online Safety team.

Student Online Safety Education

Online Safety will be covered as an integral part of the School curriculum.

Students will be taught what Internet use is acceptable and what is not and given clear objectives for internet use.

The risks of Internet usage will be explained to students, including inappropriate content, unwanted or inappropriate contact (eg grooming), and risks of inappropriate conduct (eg handling of personal information, online reputation etc).

The following list is by no means comprehensive, but student Online Safety education will cover at least the following risks amongst others:

- Not all websites are safe. Many encourage viewing but might contain programs (e.g. viruses) harmful to personal or School computers.
- Viewing of age-inappropriate material will normally be blocked, but where inadvertently encountered must be reported. Action to deliberately avoid filters or blocks to access such material is unacceptable and may result in sanctions.

- Be warned that people in chat rooms and other online environments may not be who they claim to be - they may be of a different age, gender and personality to those claimed and might have ulterior motives for engaging in chatting with young people.
- Never arrange to meet someone alone that you have met over the internet.
- Websites encouraging violence, unlawful activities, suicide and self-harm should not be accessed.
- Emails requesting details of passwords (especially for sensitive information such as bank details) are invariably 'phishing' and should be deleted and/or reported.
- Do not give personal information (including address or phone numbers) or images of yourself or friends to unknown people on the Internet, no matter how friendly of plausible they may seem.
- Remember that information posted on the internet, especially in social networking sites, can be viewed by millions.

Authorisation

All staff must read and acknowledge the 'Staff Code of Conduct' before using any school ICT resource. Online records will be kept of staff acceptance.

Parents/guardians will be asked for their consent for students' Internet access in accordance with this policy. Paper and/or email records will be kept of such consent.

Residential students will be assessed for appropriate access in accordance with their age and cognitive abilities, and individual filtering applied to their internet access.

Email

Students may only use e-mail accounts on the school system.

Students must immediately tell a member of staff if they receive offensive e-mail

Students must not reveal personal details of themselves or others in e-mail communication, or arrange to meet anyone without specific permission

Access in school to external personal e-mail accounts will normally be blocked, but may be approved by managers for specific purposes.

The forwarding of chain emails or other 'junk-mail' is not permitted.

Sending or forwarding email containing illegal or otherwise inappropriate content is strictly forbidden. In the event that such email is received, it shall immediately be reported or deleted.

Social Networking

During school hours, social networking sites and newsgroups will be blocked for both staff and students unless a specific use is approved.

Residential students may be given access to social networking sites out of school hours subject to their own individual assessment of appropriate internet access.

Students will be advised never to give out personal details of any kind which may identify them or their location. This includes advising against using apps which use GPS to disclose the location of the user.

Students will be advised not to place personal photos with any identifiable content on any social network space.

Students will be advised on security and encouraged to set passwords, deny access to unknown individuals and instructed how to block unwanted communications. Students should be encouraged to invite known friends only and deny access to others.

Students will be advised on online bullying, which includes any form of behaviour designed to hurt, offend or cause distress to other people using any form of electronic communication. If a student feels that they are the victim of online bullying, they should report the matter immediately to a member of staff

Online bullying by staff or students at VEC is unacceptable, and will result in disciplinary action or other sanctions as appropriate.

Staff shall not be ‘friends’, or communicate in any way, with students on social networking sites.

Mobile Phones and Other Mobile Devices

Mobile phones will not be used for personal use during lessons or formal school time. The sending of abusive or inappropriate text messages is forbidden.

Staff will be issued with a school phone where contact with students is required.

Staff mobile phones should be stored away at all times unless exceptional circumstances have been agreed with the Headteacher.

In order to protect students and staff, and avoid any potential for allegations of improper conduct, smart phones – or any other mobile device (including smart watches) capable of taking photographs or video - shall not be carried on the person whilst providing intimate care (even if agreed that specific staff may carry mobile phones, as mentioned previously.

Published Content and the School Web Site

Any contact details on the web site should be the school address, e-mail, telephone and fax number. Staff or students’ personal information will not be published.

Students' full names will not be used anywhere on the web site or social networking sites, particularly in association with photographs.

Written permission from parents or carers will be obtained before photographs of students are published on the school web site. Photographs will not be saved using student names as file names. (This prevents student photos being found using online search engines)

Work can only be published with the permission of the student and parents.

Data Protection

Personal data will be recorded, processed, transferred and made available in accordance with the Data Protection Act 1998. In particular, personal data must never leave the site unless encrypted, for example on an encrypted USB stick.

Handling Online Safety Complaints

Complaints of internet misuse will be dealt with by a senior member of staff.

Any complaint about staff misuse must be referred to the Hedteacher.

Complaints of a safeguarding nature must be dealt with immediately in accordance with school safeguarding procedures.

Students and parents will be informed of the complaints procedure.

Communication of Policy

Students

Students will be informed of the Online Safety rules, and that internet use will be monitored.

Staff

All staff will be given access to the Online Safety Policy and its importance explained in regular training updates, at least annually.

Parents

Parents' attention will be drawn to the Online Safety Policy and consent requested for students' internet access. The Online Safety Policy will be published on the web site.

Governors

This Online Safety policy will be brought to the attention of the Governors, and formally approved by them. There is a designated Governor assigned to support Online Safety.

Acceptable Use Policy

This acceptable use policy helps to protect students and the school by describing acceptable and unacceptable computer use.

- The school owns the computer network and can set rules for its use.
- It is a disciplinary, and potentially criminal, offence to use a computer or network for a purpose not permitted by the school.
- Irresponsible use may result in disciplinary action or the loss of network or internet access.
- Network access must be made via the user's authorised account and password, which must not be given to any other person, with the exception that, that where appropriate, staff may be made aware of student passwords to enable appropriate support.
- All network and internet use must be appropriate to education or residential as appropriate.
- Copyright and intellectual property rights must be respected.
- Messages shall be written carefully and politely, particularly as email could be forwarded to unintended readers.
- Anonymous messages and chain letters are not permitted.
- Users must take care not to reveal personal information through email, personal publishing, blogs or messaging.
- The school ICT systems may be used for reasonable private purposes (for example online banking), but such private use is not to interfere in any way with school duties.
- Use for personal financial gain, gambling, political activity, advertising or illegal purposes is not permitted.
- The school may exercise its right to monitor the use of the school's computer systems, including access to websites, the interception of e-mail and the deletion of inappropriate materials where it believes unauthorised use of the school's computer system may be taking place, or the system may be being used for criminal purposes or for storing unauthorised or unlawful text, imagery or sound.

Staff Code of Conduct

To ensure that staff are fully aware of their professional responsibilities when using information systems, they are asked to agree to this code of conduct:

- The information systems are school property and I understand that it is a disciplinary, or in extreme cases, criminal, offence to use a computer for a purpose not permitted by the school.
- I will ensure that my information systems use will always be compatible with my professional role.

- I understand that school information systems may be used for reasonable private purposes (such as online banking), but that any such use shall not affect school duties in any way.
- I understand that the school may monitor my network and internet use to ensure policy compliance.
- I will respect system security and I will not disclose any password or security information to anyone other than an appropriate system manager.
- I will not install any software or hardware without permission.
- I will ensure that personal data is kept secure and is used appropriately. Where personal data is necessarily removed from the premises, it shall always be encrypted.
- I will respect copyright and intellectual property rights.
- I will report any incidents of concern regarding children's safety to the school e-safety coordinators or the Designated Safeguarding Coordinator.
- I will ensure that any electronic communications with students are compatible with my professional role. This includes not befriending students on social media.
- I will promote e-safety with students in my care and will help them to develop a responsible attitude to system use and to the content they access or create.
- I understand that the school may exercise its right to monitor the use of the school's information systems, including internet access and interception of e-mail where it believes unauthorised use of the school's information system may be taking place, or the system may be being used for criminal purposes or for storing unauthorised or unlawful text, imagery or sound.

Student Code of Conduct

The following code of conduct will be included in the consent to be signed by parents/guardians for students' internet access:

- Students must only use their own account to access the internet.
- If using a mobile phone or tablet, they must not use their telephone internet service, but must connect to VEC's wireless network and use the filtering system provided.
- The internet must not be used to access, download, send, print, or display anything which is racist, violent, fanatical, offensive or illegal.
- Students must never give their name, home address, telephone number or provide a picture to people that they meet on the internet without permission from a member of staff.
- Students must not use any apps which use GPS to disclose their locations to others.

- The internet must not be used for bullying or anything which could give us a bad name.
- Copyright rules must be respected.
- If students find anything that they are unhappy with, or receive messages that they do not like, they must tell a member of staff immediately.
- Students' internet access will be monitored, and if these rules are broken their internet access may be restricted or stopped.

Related Policies

The following related policies are all available on the VEC intranet:

<u>VEC Policies</u>

Safeguarding (Child Protection)
Positive Behaviour Management Policy
Social Networking Policy
Anti-bullying and online bullying Policy
<u>Livability Policies</u>

Disciplinary Policy and Procedure
ICS Policy
ICT Security Procedure
Email, Internet and Computer Use Procedure

Reviewed annually or as deemed necessary.

Amy Hunt & Alina Chiuda – Online Safety Champions Andy Price – IT Manager / Simon Brown - Headteacher	April 2015
Due to be reviewed:	Reviewed: April 2016
Due for next review:	April 2017
Reviewed May 2017 by Amy Hunt.	
Reviewed: September 2017 by Amy Hunt.	

Reviewed February 2021 by Amy Hunt. Due for next review February 22.