B4L E-SAFETY AND E-SECURITY POLICY

Weston Point College

Contents

Table of Contents

1. Introduction

Weston Point College understands that computer technology is an essential resource for supporting teaching and learning. The internet, and other digital information technologies, open up opportunities for students and play an important role in their everyday lives. E-Safety encompasses Internet technologies and electronic communications such as mobile phones as well as collaboration tools and personal publishing. It highlights the need to educate students about the benefits and risks of using technology and provides safeguards and awareness for users to enable them to control their online experience. The college's e-safety policy operates in conjunction with other policies including those for Student Behaviour, Bullying and Curriculum.

The college recognises the importance of promoting the use of computer technology throughout the curriculum and understands the need for safe internet access and appropriate use. The aim of this policy is to ensure appropriate and safe use of the internet and other digital technology devices by all students and staff. Weston Point College is committed to providing a safe learning and teaching environment for all students and staff and has implemented controls to reduce any harmful risks.

This policy will be updated as required to reflect best practice, or amendments made to legislation, and will be reviewed every new academic year.

2. Considerations when using the internet

Weston Point College recognises that modern technology is an intrinsic part of modern-day life and our students use ICT extensively both within and outside of education. However, along with the opportunities that ICT offers it also brings with it problems and risks that all staff, students and parents need to be aware of.

The breadth of issues classified within online safety is considerable, but can be categorised into three areas of risk: content: being exposed to illegal, inappropriate or harmful material; contact: being subjected to harmful online interaction with other users; conduct: personal online behaviour that increases the likelihood of, or actually causes harm.

When accessing the internet, individuals are especially vulnerable to several risks which may be physically and emotionally harmful, including:

- Access to illegal, harmful or inappropriate images
- Sharing the personal information of others without the individual's consent or knowledge
- Access to, or loss of, personal information
- Cyber Bullying
- Access to unsuitable online videos and games
- Loss of personal images
- Online sexual harassment and abuse
- Inappropriate communication with others
- Illegal downloading of files
- Exposure to explicit or harmful content, e.g. involving radicalisation
- Plagiarism and copyright infringement
- Sharing the personal information with others without the individual's consent or knowledge

3. Roles and responsibilities

3.1. It is the responsibility of all users to ensure that the internet, is used in an appropriate and legal manner. If any users are witnesses to or believe that ANY illegal or harmful activities have taken, or are taking place, they MUST inform the head teacher or the Designated Safeguarding Lead immediately.

3.2. Weston Point College will ensure that the day to day management and safety of the systems and software used, including appropriate filtering, are well maintained and up to date, dealing with any issues that may arise. Particular attention will be paid when there has been a "power outage" to ensure the appropriate filtering is still in place.

- The security of the college information systems will be reviewed regularly.
- Virus protection will be installed and updated regularly.
- The college uses broadband with its firewall and filters.
- The college will work in partnership with the service provider to ensure filtering systems are as effective as possible.
- The contact details on the Web site should be the college address, e-mail and telephone number.
- Staff or students personal information will not be published.
- The Bridge4Learning Directors will take overall editorial responsibility and ensure that content of the Website is accurate and appropriate.

3.3. Comtec will provide technical support and advice to members of staff as required and will support any wider CPD.

3.4. The Head Teacher will ensure there is a system in place which monitors and supports the E-Safety and E-Security of the college and work with the Designated Safeguarding Lead (DSL) to carry out the monitoring, keeping in mind data protection requirements. Please refer to Information Sharing Protocols.

3.5. A log of any incidents and technical issues will be maintained. All incidents and issues will be reported to the Head Teacher and the Designated Safeguarding Lead (DSL).

3.6. Cyber bullying incidents will be reported in accordance with Weston Point College's Anti-Bullying Policy.

3.7. All staff are responsible for ensuring that e-safety is embedded in the curriculum and safe internet access is promoted.

3.8. All staff and students must ensure that they adhere to Weston Point College's Acceptable Use Policy. A log of acceptance will be maintained and updated as and when changes occur.

3.9. All students must be made aware of their responsibilities regarding the use of the College's ICT systems and equipment, including their expected behaviour.

3.10. Weston Point College meets with the minimum GDPR ICT Audit Requirements or better.

2..

4. E-Safety

4.1. Educating pupils:

4.1.1. The college will regularly update students to make sure they are aware of the safe use of new technology both inside and outside of the college.

4.1.2. Students will be taught about the importance of e-safety and are encouraged to be critically aware of the content they access online, including extremist material and the validity of website content.

4.1.3. Students will be taught to acknowledge information they access online, to avoid copyright infringement and/or plagiarism.

4.1.4. Clear guidance on the rules of internet use will be present in all classrooms where ICT is used.

4.1.5. Students are instructed to report any suspicious use of the internet and digital devices to a member of staff.

4.1.6. The college will hold e-safety events, such as Safer Internet Day and Anti Bullying Week, to promote online safety.

4.2. Educating staff:

4.2.1. E-safety training opportunities is available to all staff.

4.2.2. All staff will undergo e-safety training including cyber security on an annual basis to ensure they are aware of current issues and any changes to the provision of e-safety, as well as current developments in social media and the internet.

4.2.3. All staff will undergo an annual "Skills Audit" by the college that will identify individual CPD needs of staff.

4.2.4. All staff will employ methods of good practice and act as role models for students when using the internet and other digital devices.

4.2.5. All staff are reminded of the importance of acknowledging information they access online, in order to avoid copyright infringement and/or plagiarism.

4.2.6. Any new staff are required to undergo online safety and awareness training as part of their induction programme, ensuring they fully understand this policy.

4.2.7. The Head Teacher and or Deputy Heads will act as the first point of contact for staff requiring general e- safety advice. Safeguarding issues or concerns must be referred to the Designated Safeguarding Lead.

5. Control Measures

5.1. Internet access will be authorised once parents/carers and students have returned the signed consent form in line with Weston Point College's Acceptable Use Policy.

5.2. A record will be kept by the college of all students who have been granted internet access.

5.3. All users will be provided with usernames and passwords for the college's VLE and must keep these confidential to avoid any other students using their login details.

5.4. Keeping Children Safe in Education compliant filtering systems MUST be in place and in use to reduce any potential risks to pupils through access to, or trying to access, certain websites.

5.5. Any requests by staff for websites to be added or removed from the filtering list must be authorised by the Head Teacher.

5.6. A record will be kept by the college of all students who have been granted internet access.

5.7. All users will be provided with usernames and passwords for the college's VLE and must keep these confidential to avoid any other students using their login details.

5.8. Keeping Children Safe in Education compliant filtering systems MUST be in place and in use to reduce any potential risks to pupils through access to, or trying to access, certain websites which are harmful or use inappropriate material.

5.9. All the college's systems are protected by up-to-date anti-virus software

6. Social Networking

6.1. Access to social networking sites will be filtered as appropriate

6.2. Should access be needed to social networking sites for any reason this will always be monitored and controlled by staff and must be first authorised by the Head Teacher

6.3. Staff are not permitted to publish comments about Weston Point College which may affect its reputability

7. Published content on the Bridge4Learning Website

7.1. The Directors will be responsible for the overall content of the college website and will ensure the content is appropriate and accurate.

7.2. Contact details on the college website will include the email, telephone number and the address of the college.

7.3. No images, student names or any content that may identify individual students will be published on the website.

7.4. Students are not permitted to take pictures or publish them without permission of the individual and the college.

7.5. Staff can take pictures, though they must do so in accordance with the college's policies in terms of the sharing and distribution of such. Staff will not take pictures using their personal equipment unless they have received explicit permission from the Head Teacher to do so. Any such images may only be used for the express purpose they were taken for. The images will not be stored on personal equipment and will be deleted as soon as they have served their purpose.

7.6. Any member of staff who is representing the college online, via blogging, U-tube, etc. must express neutral opinions and not disclose any confidential information regarding the college or any information that may affect its reputability.

8. Mobile Devices and hand-held computers

8.1. The Head Teacher may authorise the use of mobile devices for students and staff where it is seen to be for safety, precautionary or educational use.

8.2. Using the college's devices or network to send inappropriate messages or images is prohibited.

8.3. Personal mobile devices will not be used to take images or videos of students or staff unless explicit authorisation has been mandated by the Head Teacher.

9. Cyber Bullying

This section must be reviewed alongside the college's Anti-Bullying Policy.

9.1. For the purposes of this policy, cyber bullying is a form of bullying whereby an individual is the victim of harmful or offensive posting of information or images online.

9.2. The college recognises that both staff and pupils may experience cyber bullying and will commit to preventing any instances that should occur.

9.3. The college will regularly educate staff, students, and parents/carers on the importance of staying safe online, as well as being considerate to what they post online.

9.4. The college will commit to creating a learning and teaching environment which is free from harassment and bullying, for all staff and students.

9.5. The Head Teacher, Deputy Heads and the Directors will decide whether it is appropriate to notify the police or other appropriate parties regarding the action taken against a student or staff member.

10. Reporting and Misuse

10.1. The college will clearly define what is classed as inappropriate behaviour in the Acceptable Use Policy, ensuring student and staff are aware of what behaviour is expected of them.

10.2. Inappropriate activities are discussed and the reasoning behind prohibiting activities due to e-safety are explained to students as part of the curriculum in order to promote responsible internet use.

Misuse by Students:

10.3. Any instances of misuse should be immediately reported to a member of staff, who will then report this to the Head Teacher and the Designated Safeguarding Lead.

10.4. Any student who does not adhere to the rules outlined in our Acceptable Use Policy and is found to be wilfully misusing the internet, may face sanctions as determined by the Head Teacher.

10.5. Complaints of a child protection nature, such as when a student is found to be accessing extremist material, shall be dealt with in accordance with the "Child Protection and Safeguarding Policy" and reported to the Designated Safeguarding Lead and the Head Teacher.

10.6. As a student of Weston Point College, failure to comply with any part of this policy may result in one or more of the following sanctions (in line with behaviour policy) to be faced

- Verbal warning/advice
- Enforced e-safety enrichment
- A ban, temporary or permanent, on the use of the technology facilities
- A letter/phone call informing parents/carers of the nature of the breach of rules
- A formal interview with parents/carers, the student in question and staff
- Referral to external agencies e.g. police, local authority
- Fixed Term Exclusion
- Any other action determined by the Head Teacher and/or Deputy Heads

Misuse by Staff:

10.7. Any misuse of the internet by a member of staff should be immediately reported to the Head Teacher.

10.8. The Head Teacher will deal with such incidents in accordance with the "Allegations of Abuse Against Staff Policy" and may decide to take disciplinary action against the member of staff.

10.9. The Head Teacher and Directors will decide whether it is appropriate to notify the police of the action taken against a member of staff.

Use of illegal material:

10.10. In the event that illegal material is found on any of the Bridge4Learning network, or evidence suggests that illegal material has been accessed, the college will carry out a thorough investigation with support from the Directors. Where appropriate the police will be contacted.

10.11. If a child protection incident is suspected, the college's child protection procedure will be followed - the DSL, Head Teacher and Directors will be informed, and the police contacted.

11. Physical Security and Location Access

11.1. All on site devices are kept in secure locations. Access is restricted to authorised personnel only.

11.2. Procedures are in place to ensure access is removed when no longer required.

11.3. Data back-ups are carried out routinely and stored in a fire-proof safe. Access is restricted to authorised personnel only.

11.4. Physical access to the server is restricted to authorised personnel only.

.

12. Data Processing Equipment Locations

12.1. The location for data processor screens at the college are in secure locations. Procedures are in place to ensure any possibility of the data processors screen being "over seen" is addressed before the device is used to process ANY college data.

12.2. Devices must not be left logged on for any period of time when they are unattended.

12.3. Accounts must not be shared with any other user for any reason.

12.4. Passwords must not be shared with any other user for any reason.

12.5. Users must not leave hard copies of personal or unencrypted identifiable data unattended at any time unless stored in a secure location that meets the physical security statements set out above. **NB** Unattended data or data access is considered as a Data Breach and MUST BE reported to the Head Teacher for investigation.

12.6. For clarity, the statements above must be adhered to when accessing college data from any device or from any location, such as, home, public space, friends/family homes etc. Access to data MUST be secured from other unauthorised users at all times.

13. Inventory

13.1. To meet the obligations of the Data Protection Act 2018 it is essential that ICT equipment is secure, the college maintains and keeps an up to date audit of ICT equipment.

14. Data Back-up

14.1. All data must be backed up to secure and GDPR Location. The college's data is stored in a fire-proof safe.

14.2. The data stored complies with the college's data retention policy.

14.3. The back-up regime allows for any individual piece of data to be recovered in a timely manner. It is accepted that some degree of data loss may incur but this does not exceed more than data produced over the last 24 hours.

14.4. Users may back up their data individually, but this back-up must meet the required data security principles in this document.

14.5. The primary back-ups are carried out by Comtec at set intervals and information contained within these back-ups are only accessible by Comtec for verification and restoration. Other back-up methods can be used to allow users direct self- recovery of files in addition to a "Primary Back-up" but all backups must meet the storage and security requirements set out in this document.

15. Malware and Virus Detection and Removal

15.1. Malware (malicious software) and Viruses can infiltrate systems and software and cause damage or allow systems to be used for malicious or unlawful activities.

15.2. All college devices MUST Use Anti-virus / Anti-malware detection and removal software at all times. This software MUST be set to scan on access for all devices and updates as a minimum of monthly. Where possible the software must be configured in such a way to stop unauthorised users from disabling it.

15.3. Users MUST NOT disable any Anti-virus/Anti-Malware software installed on their machine for any reason. If the user has an issue that they believe requires this to happen then they MUST contact Comtec for support.

15.4. Mobile devices including college and personal laptops and mobile phones must be encrypted and password protected.

15.5. Please note that device accounts are for an individual's use and must not be shared. If Another user requires access to the device this MUST be done using an appropriate account for the users and ensure that the user cannot access any data that they are not officially authorised to access.

15.6. All works devices MUST be encrypted, and password protected. When using mobile phones users must be aware of their surroundings and the ability to be "overheard" when discussing personal identifiable information.

15.7. Any device that is used to access or Store College data including contact information or emails MUST be password protected as a minimum.

15.8. If this device is shared with other people outside of the college staff, then the device MUST be set in such a way that the data is not accessible by the other users. As this data is classed as offsite this data MUST be encrypted.

15.9. Mobile Phones and Tablets MUST be kept up to date with Apps and Operating Systems. It is the college's responsibility to ensure this is carried out for all college owned devices. Users MUST ensure that their device meets this requirement.

16. Protecting data with passwords

16.1. All accounts MUST be password protected:

16.2. Passwords must be changed frequently (minimum every 12 months) or immediately if you suspect someone has obtained your password or you believe it may have been compromised.

16.3. Passwords MUST NOT be shared with other users.

17. Patch and Software Updates

The college keeps all device software and hardware up to date. Comtec manages and installs the updates. ALL critical updates and patches that are issued by hardware and software vendors are implemented as a matter of urgency.

18. Policy review

This policy is reviewed every year by the Head Teacher

Issue Date: 01/11/2020

The next review date for this policy is October 2021.