William Brookes Academy Trust

E-Safety Policy

September 2019

E-Safety Policy
William Brookes Academy Trust
September 2019

This policy is due for review in 12 months

Statement of Intent

At William Brookes School, we understand that computer technology is an essential resource for supporting teaching and learning. The internet, and other digital and information technologies, open up opportunities for students and play an important role in their everyday lives.

Whilst the school recognises the importance of promoting the use of computer technology throughout the curriculum, we also recognise the need for safe internet access and appropriate use.

Our school has created this policy with the aim of ensuring appropriate and safe use of the internet and other digital technology devices by all students and staff.

The school is committed to providing a safe learning and teaching environment for all students and staff and has implemented important controls to prevent any harmful risks.

This policy will operate in conjunction with other important policies in our school, including our:

- Anti-bullying Policy
- Data Protection Policy
- Child Protection and Safeguarding Policy
- Cyber Bullying Policy
- Whistleblowing Policy & Procedure
- Digital Devices Responsible Use Policy (issued to students and parents)
- Acceptable Use Policy

1. Legal framework

1.1 This policy has due regard to the following legislation, including, but not limited to:

- The Human Rights Act 1998
- General Data Protection Regulation, The Data Protection Act 2018
- The Safeguarding Vulnerable Groups Act 2006
- The Education and Inspection Act 2006
- The Computer Misuse Act 1990, amended by the Police and Justice Act 2006
- The Freedom of Information Act 2000
- The DfE's Keeping Children Safe in Education policy [New/updated for 2019]

2. Use of the internet

2.1 The school understands that using the internet is important when raising educational standards, promoting student achievement and enhancing teaching and learning.

2.2 Internet use is embedded in the statutory curriculum and is therefore entitled to all students, though there are a number of controls required for schools to implement, which minimise harmful risks.

2.3 When accessing the internet, individuals are especially vulnerable to a number of risks which may be physically and emotionally harmful. These risks include:

- Access to illegal, harmful or inappropriate images
- Cyber bullying
- Access to, or loss of, personal information
- Access to unsuitable online videos or games
- Loss of personal images
- Inappropriate communication with others
- Illegal downloading of files
- Plagiarism and copyright infringement
- Sharing the personal information of others without the individual's consent or knowledge
- Exposure to explicit or harmful content, eg, radicalisation [New/updated for 2019]

3. Roles and responsibilities

3.1 It is the responsibility of all staff to be alert to possible harm to students or staff, due to inappropriate internet access or use both inside and outside of the school, and to deal with incidents of such as a priority.

3.2 The governing board is responsible for ensuring that there are appropriate filtering and monitoring systems in place to safeguard students.

3.3 The Assistant Head Teacher/DSL with responsibility for Behaviour is responsible for ensuring the day-to-day e-safety in our school and managing any issues.

3.4 The head teacher is responsible for ensuring that all relevant staff receive continuous professional development to allow them to fulfil their role and train other members of staff.

3.5 The DSL will provide all relevant training and advice for members of staff as part of the requirement for staff to undergo regularly updated safeguarding training and be able to teach students about online safety.

3.6 The head teacher and data protection officer (DPO) will ensure there is a system in place which monitors and supports the DSL whose role is to carry out the monitoring of e-safety in the school, keeping in mind data protection requirements.

3.7 The head teacher will ensure there is a system in place which monitors and supports the DSL, whose role is to carry out the monitoring of e-safety in the school.

3.8 The DSL will regularly monitor the provision of e-safety in the school and return this to the head teacher.

3.9 The school has a procedure for reporting incidents and inappropriate internet use, either by students or staff.

3.10 Cyber bullying incidents will be reported in accordance with the school's Anti-Bullying Policy.

3.11 The DSL will ensure that all members of staff are aware of the procedure when reporting e-safety incidents and will keep a log of all incidents recorded.

3.10 The governing body will hold meetings with the DSL to discuss the effectiveness of the e-safety provision, current issues, and to review incident logs.

3.11 The governing body will evaluate and review this E-safety Policy on an annual basis.

3.12 The head teacher will review and amend this policy with the safeguarding lead, taking into account new legislation and government guidance, and previously reported incidents to improve procedures.

3.13 Teachers are responsible for ensuring that e-safety issues are embedded in the curriculum and safe internet access is promoted at all times.

3.14 All staff are responsible for ensuring they are up-to-date with current e-safety issues, and this E-safety Policy.

3.15 All staff and students will ensure they understand and adhere to the Acceptable Use Policy. Students are to return a signed copy to the ICT support team and staff to the Head's Office by way of their completed Induction Feedback Form.

3.16 Parents/carers are responsible for ensuring their child understands how to use computer technology and other digital devices, appropriately.

3.17 Smoothwall email logs are checked daily by the Network Manager. Details of any safe guarding or child protection concerns detected are noted on a Concern Referral Form and investigated.

4. E-safety control measures

4.1 Educating students:

- An e-safety programme is taught across the curriculum on a regular basis, ensuring students are aware of the safe use of new technology both inside and outside of the school.
- 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.
- Students will be taught to acknowledge information they access online, in order to avoid copyright infringement and/or plagiarism.
- Students are instructed to report any6 suspicious use of the internet and digital devices to their classroom teacher.
- PSHE lessons will be used to educate students about cyber bullying, including how to report cyber bullying, the social effects of spending too much time online and where to access help.
- The school will hold e-safety events, such as Safer Internet Day and Anti-Bullying Week to promote online safety.

4.2 Educating staff:

- All staff will undergo e-safety training and updates as and when required to ensure they are aware of current e-safety issues and any changes to the provision of e-safety.
- All staff will employ methods of good practice and act as role models for students when using the internet and other digital devices.
- Any new staff are required to undergo e-safety training as part of their induction programme, ensuring they fully understand the E-safety Policy.
- All staff are reminded of the importance of acknowledging information they access online, in order to avoid copyright infringement and/or plagiarism.

4.3 Internet access:

- Internet access will be authorised once students have signed the consent form as part of the Acceptable Use Policy.
- A record will be kept by the ICT support team of all students who have been granted internet access.
- All users will be provided with usernames and passwords, and are advised to keep this confidential to avoid any other students using their login details.
- Students' passwords will be changed on a regular basis, and their activity is continuously monitored by the safeguarding lead.
- Management systems will be in place to allow teachers and members of staff to control workstations and monitor students' activity.
- Effective filtering systems will be established to minimise any potential risks to students through access to particular websites.
- Any requests by staff for websites to be added or removed from the filtering list must be first authorised by the head teacher.
- All school systems will be protected by up-to-date virus software.
- An agreed procedure will be in place for the provision of temporary users, e.g. volunteers.
- The admin users' passwords will be available to the head teacher for regular monitoring of activity.

- Staff are able to use the internet for personal use during out-of-school hours as well as break and lunchtimes.
- Personal use will only be monitored by the ICT support team for access to any inappropriate or explicit sites, where the need to do so outweighs the need for privacy.
- Inappropriate internet access by staff may result in the staff member being permitted to use the internet for school purposes only and prohibited from using any personal devices. This will be dealt with following the process outlined in the misuse by staff section of this policy.

4.4 Email:

- Students and staff will be given approved email accounts and are only able to use these accounts for work related activities.
- The use of personal email accounts to send and receive personal data or information is prohibited.
- No sensitive personal data shall be sent to any other students, staff or third parties via email.
- Students are made aware that all email messages are monitored and that the filtering system will detect inappropriate links, viruses, malware and profanity.
- Chain letters, spam and all other emails from unknown sources will be deleted without opening.

4.5 Social networking:

- The use of social media on behalf of the school will be conducted following the processes outlined in our Social Media Policy.
- Access to social networking sites will be filtered as appropriate.
- Should access be needed to social networking sites for any reason, this will be monitored and controlled by staff at all times and must be first authorised by the head teacher.
- Students are regularly educated on the implications of posting personal data online, outside of the school.
- Staff are educated on posting inappropriate photos or information online, which may potentially affect their position and the school as a whole.
- Staff are not permitted to communicate with students over social networking sites.
- Staff are not permitted to publish comments about the school which may affect its reputation.
- Staff are not permitted to access social media sites during teaching hours unless it is beneficial to the material being taught. This will be discussed with the head teacher prior to accessing the social media site.

4.6 Published content on the school website and images:

- The head teacher will be responsible for the overall content of the website, and will ensure the content is appropriate and accurate.
- All contact details on the school website will be the phone, email and address of the school. No personal details of staff or students will be published.
- Images and full names of students, or any content that may easily identify a student, will be selected carefully, and will not be posted until authorisation from parents has been received.
- Students are not permitted to take or publish photos of others without permission from the individual.
- Staff are able to take images, though they must do so in accordance with school policies in terms of the sharing and distribution of such. Staff will not take images using their personal equipment.

4.7 Mobile devices and hand-held computers:

- Students in Years 7-11 are prohibited from using a mobile phone in school between 08.45 and 15.15 hours.
- The headteacher may authorise the use of mobile devices by a student where it is seen to be for safety or precautionary use.
- Students are not permitted to access the school's Wi-Fi system at any time using their mobile phones.
- Staff are permitted to use hand-held computers which have been provided by the school, though internet access will be monitored for any inappropriate use by the ICT support team where it is justifiable to do so and the justification outweighs the need for privacy.
- The sending of inappropriate messages or images from mobile devices is prohibited.
- Mobile devices must not be used to take images of students or staff.
- The DPO will, in collaboration with the ICT support team, ensure all school-owned devices are password protected.
- The ICT support team will review all mobile devices and hand-held computers on a termly basis to ensure all apps are compliant with tata protection regulations and up-to-date and to carry out any required updates.
- The ICT support team and DSL will review and authorise any apps and/or computer programmes before they are download. No apps or programmes will be downloaded without express permission from an ICT support team member or the DSL
- Apps will only be downloaded from manufacturer approved stores, eg, Google Play and the Apple App Store.

4.8 Network security

- Network profiles for each student and staff member are created in which the individual must enter a username and personal password when accessing the ICT systems within the school.
- Password have a minimum and maximum length, to prevent "easy" passwords or mistakes when creating passwords.
- Passwords will expire after 60 days to ensure maximum security for student and staff accounts.
- Passwords should be stored using non-reversible encryption.

- The ICT support team and DSL will ensure all school-owned laptops and computers have their encryption settings turned on when installed.
- Important folders, eg, those including student medical records, will be password protected to ensure their security – only designated individuals will have access to this password.

4.9 Virus management

- Technical security features, such as virus software, are kept up-to-date and managed by the ICT support team.
- The ICT support team will ensure that the filtering of websites and downloads is up-to-date and monitored.
- Firewalls will be switched on at all times. The ICT support team will review these on a weekly basis to ensure they are running correctly and will carry out any required updates.
- Firewalls and other virus management systems, eg, anti-virus software, will be maintained in accordance with the school's policy.
- Staff members will report all malware and virus attacks to the ICT support team.

5. Cyber bullying

5.1 For the purpose 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.

5.2 The school recognises that both staff and students may experience cyber bullying and is committed to responding appropriately to any instances that should occur.

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

5.4 Students will be educated about online safety through teaching and learning opportunities as part of a broad and balanced curriculum; this includes covering relevant issues within PSHE lessons as well as sex and relationship education.

5.5 The school will commit to creating a learning and teaching environment which is free from harassment and bullying, ensuring the happiness of all members of staff and students.

5.6 The school has zero tolerance for cyber bullying, and any incidents will be treated with the upmost seriousness and dealt with in accordance with our Anti-bullying Policy and Cyber Bullying Policy.

5.7 The head teacher will decide whether it is appropriate to notify the police or anti-social behaviour coordinator in their LA of the action taken against a student.

6. Reporting misuse

6.1 The school will clearly define what is classed as inappropriate behaviour in the Acceptable Use Agreement, ensuring all students and staff members are aware of what behaviour is expected of them.

6.2 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.

6.3 Misuse by students:

- Teachers have the power to discipline students who engage in misbehaviour with regards to internet use.
- Any instances of misuse should be immediately reported to a member of staff.
- Any student who does not adhere to the rules outlined in our Acceptable Use Policy and is found to be wilfully misusing the internet, will have a letter sent to their parents/carers explaining the reason for suspending their internet use.
- Members of staff may decide to issue other forms of disciplinary action to a student upon the misuse of the internet. This will be discussed with the head teacher and will be issued once the student is on the school premises.
- Complaints of a child protection nature shall be dealt with in accordance with our Child Protection Policy.

6.4 Misuse by staff:

- Any misuse of the internet by a member of staff should be immediately reported to the head teacher.
- The headteacher will deal with such incidents in accordance with the school's Safeguarding & Child Protection and Whistleblowing Policies & Procedures and may decide to take disciplinary action against the member of staff.
- The head teacher will decide whether it is appropriate to notify the police or anti-social behaviour coordinator in their LA of the action taken against a member of staff.

6.5 Use of illegal material:

- In the event that illegal material is found on the school's network, or evidence suggests that illegal material has been accessed, the police will be contacted.
- The incident will be immediately reported to the police if the illegal material is, or is suspected to be, a child sexual abuse image hosted anywhere in the world, a non-photographic child sexual abuse images hosted in the UK, or criminally obscene adult content hosted in the UK.
- If a child protection incident is suspected, the school's Safeguarding and Child Protection procedure will be followed.
- Staff will not view or forward illegal images of a child. If they are made aware of such an image, they are to contact the DSL.

7. Monitoring and Review

7.1 This policy is reviewed annually by the Assistant Head Teacher/DSL with responsibility for Behaviour and the head teacher.

7.2 Any changes made to this policy by the head teacher and Assistant Head Teacher/DSL with responsibility for Behaviour will be communicated to all members of staff.

7.3 All members of staff are required to familiarise themselves with all processes and procedures outlined in this policy as part of their induction programme.

7.4 The next scheduled review date for this policy is September 2020