NORTON COLLEGE
WORCESTER

E-Safety Policy

Statement of intent

At Norton College, 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 College recognises the importance of promoting the use of computer technology throughout the curriculum, we also understand the need for safe internet access and appropriate use.

Our College 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 College is committed to providing a safe learning and teaching environment for all students and staff, and has implemented important controls to mitigate the risk of harm.

Approved by: ___Luke Goold___________ Date: _01/09/2020___

Chair of Directors___Edward Morris_____ Date: _01/09/2020__

Review Date: _01.09.2021___

1. Legal framework

1.1 This policy has due regard to all relevant legislation including, but not limited to:

- The General Data Protection Regulation
- Freedom of Information Act 2000

1.2 This policy also has regard to the following statutory guidance:

- Department for Education (DfE) (2019) ‘Keeping children safe in education’
- National Cyber Security Centre (2017) ‘Cyber Security: Small Business Guide’

1.3 This policy will be used in conjunction with the following College policies and procedures:

- E-security Policy
- Digital Safeguarding Policy
- Cyber Bullying Policy
- Social Media Policy
- Allegations of Abuse Against Staff Policy
- Acceptable Use Agreement
- Data Security Breach Prevention and Management Plan

2. Use of the internet

2.1 The College 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 an entitlement for all students, though there are a number of controls the College is required to implement to 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, including the following:

- 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
- Exposure to explicit or harmful content, e.g. content involving radicalisation
- Plagiarism and copyright infringement
- Sharing the personal information of others without the individual’s consent or knowledge

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 College, and to deal with incidents of such as a priority.

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

3.3 The e-safety officer, is responsible for ensuring the day-to-day e-safety in College and managing any issues that may arise.

3.4 The Acting Head of school is responsible for ensuring that the e-safety officer and any other relevant staff receive Continuing Professional Development Training (CPD) to allow them to fulfil their role and train other members of staff.

3.5 The Designated Safeguard Lead (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 Acting Head of school will ensure there is a system in place which monitors and supports the e-safety officer, whose role is to carry out the monitoring of e-safety in College, keeping in mind data protection requirements.

3.7 The e-safety officer will regularly monitor the provision of e-safety in the College using the DNA software and will provide feedback to the Acting Head of school.

3.8 The Acting Head of school will establish a procedure for reporting incidents and inappropriate internet use, either by students or staff.

3.9 The e-safety officer 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 e-safety officer will attempt to find alternatives to monitoring staff use of social media, where possible, and will justify all instances of monitoring to ensure that it is necessary and outweighs the need for privacy. The member of staff who is being monitored will be consulted prior to any interception by the College.

3.11 The board of directors will hold regular meetings with the e-safety officer to discuss the effectiveness of the e-safety provision, current issues, and to review incident logs, as part of the College's duty of care.

3.12 The board of directors will evaluate and review this E-safety Policy on an annual basis, considering the latest developments in ICT and the feedback from staff/students.

3.13 The Acting Head of school will review and amend this policy with the e-safety officer, taking into account new legislation, government guidance and previously reported incidents, to improve procedures.

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

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

3.16 All staff and students will ensure they understand and adhere to our Acceptable Use Agreement, which they must sign and return to the Acting Head of school.

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

3.18 The Acting Head of school is responsible for communicating with parents/carers regularly and updating them on current e-safety issues and control measures.

3.19 All students are aware of their responsibilities regarding the use of College based ICT systems and equipment, including their expected behaviour.

4. E-safety education

4.1 An e-safety programme will be established and taught across the curriculum on a regular basis, ensuring that students are aware of the safe use of new technology both inside and outside of the College.

4.2 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.

4.3 Students will be taught to acknowledge ownership of information they access online, in order to avoid copyright infringement and/or plagiarism.

4.4 Clear guidance on the rules of internet use will be presented in all classrooms.

4.5 Students are instructed to report any suspicious use of the internet and digital devices to the senior management team (SMT)

4.6 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.

4.7 The College will hold e-safety events, such as Safer Internet Day and AntiBullying Week, to promote online safety.

4.8 A planned calendar programme of e-safety training opportunities is available to all staff members, including whole College activities and CPD training courses.

4.9 All staff will undergo e-safety training on a termly basis to ensure they are aware of current e-safety issues and any changes to the provision of e-safety, as well as current developments in social media and the internet as a whole.

4.10 All staff will undergo regular audits by the e-safety officer in order to identify areas of training need.

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

4.12 All staff will be educated on which sites are deemed appropriate and inappropriate.

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

4.14 Any new staff are required to undergo e-safety training as part of their induction programme, ensuring they fully understand this E-safety Policy.

4.15 The e-safety officer will act as the first point of contact for staff requiring e-safety advice.

4.16 E-safety information will be directly delivered to parents through a variety of formats, including newsletters, the College website and social media.

4.17 Twilight courses and presentations will be run by the College for parents.

4.18 Parent/carers' evenings, meetings and other similar occasions will be utilised to inform parents of any e-safety related concerns.

5. E-safety control measures

5.1 Internet access will be authorised once parents/carers and students have returned the signed consent form in line with our Acceptable Use Agreement.

5.2 Where a student is over the age of 13 and they fully understand what they are consenting to, parents'/carers' consent is not required in line with the GDPR; however, the College will notify parents/carers that the student has consented independently.

5.3 A record will be kept by the Head of school of all students who have been granted internet access.

5.4 All users will be provided with usernames and passwords and will be instructed to keep these confidential to avoid any other students using their login details.

5.5 Students' passwords will expire every 90 days, and their activity is continuously monitored by the e-safety officer.

5.6 Management systems will be in place to allow teachers and members of staff to control workstations and monitor students' activity.

5.7 Effective filtering systems will be established to eradicate any potential risks to students through access to, or trying to access, certain websites which are harmful or use inappropriate material.

5.8 Filtering systems will be used which are relevant to students’ age ranges, their frequency of use of ICT systems, and the proportionality of costs compared to risks.

5.9 The board of directors will ensure that the use of appropriate filters and monitoring systems does not lead to ‘over blocking’ – unreasonable restrictions as to what students can be taught with regards to online teaching and safeguarding.

5.10 Any requests by staff for websites to be added or removed from the filtering list must be first authorised by the Acting Head of school and the e-safety officer.

5.11 All College systems will be protected by up-to-date virus software.

5.12 An agreed procedure will be in place for the provision of temporary users, e.g. volunteers.

5.13 Using the DNA software, the e-safety officer will undertake regular monitoring of activity.

5.14 Staff are able to use the internet for personal use during out-of-College hours, as well as break and lunch times.

5.15 Personal use will only be monitored by the e-safety officer for access to any inappropriate or explicit sites, where the need to do so outweighs the need for privacy.

5.16 Inappropriate internet access by staff may result in the staff member being permitted to use the internet for College 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.

5.17 Students and staff will be given approved email accounts and are only able to use these accounts.

5.18 The use of personal email accounts to send and receive personal data or information is prohibited.

5.19 No sensitive personal data shall be sent to any other students, staff or third parties via email.

5.20 Students are made aware that all email messages are monitored and that the filtering system will detect inappropriate links, viruses, malware and profanity.

5.21 Staff members are aware that their email messages are not monitored.

5.22 Any emails sent by students to external organisations will be overseen by their class teacher and must be authorised before sending.

5.23 Chain letters, spam and all other emails from unknown sources will be deleted without opening.

5.24 The staff will, at the start of each College year, explain to students what a phishing email might look like –this will include information on the following:

- Determining whether or not an email address is legitimate
- Knowing the types of address, a phishing email could use
- Asking "does it urge the recipient to act immediately?"
- Checking the spelling and grammar

5.25 Staff will not be punished if they are caught out by cyber-attacks as this may prevent similar reports in the future. The e-safety officer will conduct an investigation; however, this will be to identify the cause of the attack, any compromised data and if there are any steps that can be taken in the future to prevent similar attacks happening.

5.26 The use of social media on behalf of the College will be conducted following the processes outlined in our Social Media Policy.

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

5.28 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 Acting Head of school.

5.29 Students are regularly educated on the implications of posting personal data online outside of the College.

5.30 Staff are regularly educated on posting inappropriate photos or information online, which may potentially affect their position and the College as a whole.

5.31 Staff are not permitted to communicate with students over social networking sites and are reminded to alter their privacy settings.

5.32 Staff are not permitted to publish comments about the College which may affect its reputation.

5.33 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 Acting Head of school prior to accessing the social media site.

5.34 The Acting Head of school will be responsible for the overall content of the website and will ensure the content is appropriate and accurate.

5.35 Contact details on the College website will include the phone number, email and address of the College – no personal details of staff or students will be published.

5.36 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.

5.37 Students are not permitted to take or publish photos of others without permission from the individual.

5.38 Staff are able to take pictures, though they must do so in accordance with our Photography Policy. Staff will not take pictures using their personal equipment.

5.39 Any member of staff that is representing the College online, e.g. through blogging, must express neutral opinions and not disclose any confidential information regarding the College, or any information that may affect its reputability.

5.40 The Acting Head of school may authorise the use of mobile devices by a student where it is seen to be for safety or precautionary use.

5.41 Students are not permitted to access the College's Wi-Fi system at any time using their mobile devices and hand-held computers.

5.42 Mobile devices are not permitted to be used during College hours by students or members of staff.

5.43 Staff are permitted to use hand-held computers which have been provided by the College, though internet access will be monitored for any inappropriate use by the e-safety officer where it is justifiable to do so and the justification outweighs the need for privacy.

5.44 The sending of inappropriate messages or images from mobile devices is prohibited.

5.45 Mobile devices will not be used to take images or videos of students or staff.

5.46 No mobile device or hand-held computer owned by the College will be used to access public Wi-Fi networks. ICT technicians will inform students and staff members of this rule before they can use College-owned devices away from the premises.

5.47 The e-safety office and the Acting Head of school, ensure all College-owned devices are password protected – these passwords will be changed after each use to ensure their security.

5.48 All mobile devices and hand-held computers will be fitted with tracking software to ensure they can be retrieved if lost or stolen.

5.49 To protect, retrieve and erase personal data, all mobile devices and hand-held computers will be fitted with software to ensure they can be remotely accessed.

5.50 ICT technicians will review all mobile devices and hand-held computers on a monthly basis to ensure all apps are compliant with data protection regulations and up-to-date, and to carry out any required updates.

5.51 ICT technicians and the e-safety officer will review and authorise any apps and/or computer programmes before they are downloaded – no apps or programmes will be downloaded without express permission from an ICT technician or the e-safety officer.

5.52 Apps will only be downloaded from manufacturer approved stores, e.g. Google Play and the Apple App Store.

5.53 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 College.

5.54 Passwords have a minimum and maximum length, to prevent ‘easy’ passwords or mistakes when creating passwords.

5.55 Passwords will require a mixture of letters, numbers and symbols to ensure they are secure as possible.

5.56 Passwords will expire after 90 days to ensure maximum security for student and staff accounts.

5.57 Passwords should be stored using non-reversible encryption.

5.58 The following passwords will not be accepted by the College’s security systems as they are too predictable:

- Password
- Pa55word
- Password123
- Qwerty
- 123456
- 12345678
- ABC123

5.59 The e-safety officer and ICT technicians will ensure all College-owned laptops and computers have their encryption settings turned on or, if there is no built-in encryption option, encryption software is installed.

5.60 Important folders, e.g. those including students’ medical records, will be password protected to ensure their security – the e-safety officer, and other designated individual(s) will be the only people who have access to this password.

5.61 Technical security features, such as virus software, are kept up-to-date and managed by the ICT technicians.

5.62 The e-safety officer will ensure that the filtering of websites and downloads is up-to-date and monitored.

5.63 Firewalls will be switched on at all times – ICT technicians will review these on a weekly basis to ensure they are running correctly and to carry out any required updates.

5.64 Firewalls and other virus management systems, e.g. anti-virus software, will be maintained in accordance with the College's Data Security Breach Prevention and Management Plan.

5.65 Staff members will report all malware and virus attacks to the e-safety officer and the Acting Head of school immediately.

6. Cyber bullying

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

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

6.3 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.

6.4 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.

6.5 The College 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.

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

6.7 The Acting Head of school 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.

7. Reporting misuse

7.1 Norton College 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.

7.2 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.

7.3 The Acting Head of school has the power to discipline students who engage in misbehaviour with regards to internet use.

7.4 Any instances of misuse should be immediately reported to a member of staff, who will then report this to the Acting Head of school using a complaints form.

7.5 Any student who does not adhere to the rules outlined in our Acceptable Use Agreement 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.

7.6 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 Acting Head of school and will be issued once the student is on the College premises.

7.7 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 our Child Protection and Safeguarding Policy.

7.8 Any misuse of the internet by a member of staff should be immediately reported to the Acting Head of school, using a complaints form.

7.9 The Acting Head of school 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.

7.10 The Acting Head of school 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.

7.11 In the event that illegal material is found on the College's network, or evidence suggests that illegal material has been accessed, the police will be contacted.

7.12 Incidents will be immediately reported to the Internet Watch Foundation and the police will be contacted 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 image hosted in the UK, or criminally obscene adult content hosted in the UK.

7.13 If a child protection incident is suspected, the College's child protection procedure will be followed – the DSL and Acting Head of school will be informed and the police contacted.

7.14 Staff will not view or forward illegal images of a child. If they are made aware of such an image, they will contact the DSL.

8. Monitoring and review

8.1 This policy will also be reviewed on an annual basis by the board of directors; any changes made to this policy will be communicated to all members of staff.

8.2 Members of staff are required to familiarise themselves with this policy as part of their induction programmes