Norton College (Worcester) Limited and Norton College Tewkesbury) Limited, (the College)

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.

Date policy last reviewed:	15.11.21		
Date for next review:	(Annually)		
Signed by:			
R Kenny	Executive Headteacher	Date:	15.11.21
J Powell	Board of Directors	Date:	15.11.21

1. Legal framework

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

- Voyeurism (Offences) Act 2019
- The UK General Data Protection Regulation (UK GDPR)
- Data Protection Act 2018
- DfE (2021) 'Harmful online challenges and online hoaxes'
- DfE (2021) 'Keeping children safe in education 2021'
- Department for Digital, Culture, Media and Sport and UK Council for Internet Safety (2020) 'Sharing nudes and semi-nudes: advice for education settings working with children and young people'
- DfE (2019) 'Teaching online safety in school'
- DfE (2018) 'Searching, screening and confiscation'
- National Cyber Security Centre (2018) 'Small Business Guide: Cyber Security'
- UK Council for Child Internet Safety (2020) 'Education for a Connected World – 2020 edition'

2. Roles and responsibilities

2.1 The Board of Directors is responsible for:

- Ensuring that this policy is effective and complies with relevant laws and statutory guidance.
- Ensuring the DSL's remit covers online safety.
- Ensuring their own knowledge of online safety issues is up-to-date.
- Ensuring all staff undergo safeguarding and child protection training, including online safety, at induction.
- Ensuring that there are appropriate filtering and monitoring systems in place.

2.2 The Head of School is responsible for:

- Ensuring that online safety is a running and interrelated theme throughout the College's policies and procedures, including in those related to the curriculum, teacher training and safeguarding.
- Supporting the DSL and the deputy DSL by ensuring they have enough time and resources to carry out their responsibilities in relation to online safety.
- Ensuring staff receive regular, up-to-date and appropriate online safety training and information as part of their induction and ongoing safeguarding training.
- Ensuring online safety practices are audited and evaluated.
- Supporting staff to ensure that online safety is embedded throughout the curriculum so that all students can develop an appropriate understanding of online safety.

2.3 The DSL is responsible for:

- Taking the lead responsibility for online safety in the College.
- Acting as the named point of contact within the College on all online safeguarding issues.
- Liaising with relevant members of staff on online safety matters.
- Ensuring online safety is recognised as part of the College's safeguarding responsibilities and that a coordinated approach is implemented.
- Ensuring safeguarding is considered in the College's approach to remote learning.
- Ensuring appropriate referrals are made to external agencies, as required.
- Keeping up-to-date with current research, legislation and online trends.
- Establishing a procedure for reporting online safety incidents and inappropriate internet use, both by students and staff.

- Monitoring online safety incidents to identify trends and any gaps in the College's provision, and using this data to update the school's procedures.
- Reporting to the Board of Directors about any online safety concerns through the SLT minutes.

2.4 All staff members are responsible for:

- Taking responsibility for the security of ICT systems and electronic data they use or have access to.
- Modelling good online behaviours.
- Maintaining a professional level of conduct in their personal use of technology.
- Having an awareness of online safety issues.
- Ensuring they are familiar with, and understand, the indicators that students may be unsafe online.
- Reporting concerns to the DSL.
- Where relevant to their role, ensuring online safety is embedded in their teaching of the curriculum.

2.5 Students are responsible for:

- Adhering to the Acceptable Use Agreement.
- Seeking help from College staff if they are concerned about something they or a peer have experienced online.
- Reporting online safety incidents and concerns to a member of College staff.

3. Managing online safety

3.1 All staff will be aware that technology is a significant component in many safeguarding and wellbeing issues affecting young people, particularly owing to the rise of social media and the increased prevalence of children using the internet.

3.2 The DSL has overall responsibility for the College's approach to online safety, with support from the Head of School where appropriate, and will ensure that there are strong processes in place to handle any concerns about students' safety online.

3.3 The importance of online safety is integrated across all school operations in the following ways:

- Staff receive regular training
- Online safety is integrated into learning throughout the curriculum
- DNA monitoring system is used, checked daily by the DSL to ensure no inappropriate sites are accessed or students can be referred to relevant support mechanisms.
- A firewall system is in place to ensure inappropriate sites are blocked.

3. Online safety and the curriculum

3.1 Online safety is embedded throughout the curriculum; however, it is particularly addressed in the following subjects:

- RSE
- Health education
- PSHE
- ICT

3.2 Online safety teaching is always appropriate to student' ages and developmental stages. Students are taught the underpinning knowledge and behaviours that can help them to navigate the online world safely and confidently regardless of the device, platform or app they are using. The underpinning knowledge and behaviours students learn through the curriculum include the following:

- How to evaluate what they see online

- How to recognise techniques used for persuasion
- What healthy and respectful relationships, including friendships, look like
- Body confidence and self-esteem
- Consent, e.g. with relation to the sharing of indecent imagery or online coercion to perform sexual acts
- Acceptable and unacceptable online behaviour
- How to identify online risks
- How and when to seek support
- How to identify when something is deliberately deceitful or harmful
- How to recognise when something they are being asked to do puts them at risk or is age-inappropriate

3.3 The College recognises that, while any student can be vulnerable online, there are some students who may be more susceptible to online harm or have less support from family and friends in staying safe online, e.g. pupils with SEND and LAC. Relevant members of staff, e.g. the designated teacher for LAC, work to ensure the curriculum is tailored so these students receive the information and support they need.

3.4 Before conducting a lesson or activity on online safety, the teacher/tutor will consider the topic that is being covered and the potential that students have suffered or may be suffering from online abuse or harm in this way.

3.5 If a staff member is concerned about anything students raise or disclose during online safety lessons and activities, they will make a report to the DSL.

4. Cyberbullying

4.1 Cyberbullying can include the following:

- Threatening, intimidating or upsetting text messages
- Threatening or embarrassing pictures and video clips sent via mobile phone cameras
- Silent or abusive phone calls or using the victim's phone to harass others, to make them think the victim is responsible
- Threatening or bullying emails, possibly sent using a pseudonym or someone else's name
- Menacing or upsetting responses to someone in a chatroom
- Unpleasant messages sent via instant messaging
- Unpleasant or defamatory information posted to blogs, personal websites and social networking sites, e.g. Facebook

4.2 Cyberbullying against students or staff is not tolerated under any circumstances. Incidents of cyberbullying are dealt with quickly and effectively wherever they occur in line with the Anti-bullying Policy.

5. Peer-on-peer sexual abuse and harassment

5.1 Students may also use the internet and technology as a vehicle for sexual abuse and harassment. Staff will understand that this abuse can occur both in and outside of College and off and online, and will remain aware that students are less likely to report concerning online sexual behaviours, particularly if they are using websites that they know adults will consider to be inappropriate for their age.

5.2 The following are examples of online harmful sexual behaviour of which staff will be expected to be aware:

- Threatening, facilitating or encouraging sexual violence
- Upskirting, i.e. taking a picture underneath a person's clothing without consent and with the intention of viewing their genitals, breasts or buttocks
- Sexualised online bullying, e.g. sexual jokes or taunts

- Unwanted and unsolicited sexual comments and messages
- Consensual or non-consensual sharing of sexualised imagery

5.3 Staff will be aware that creating, possessing, and distributing indecent imagery of other children, i.e. individuals under the age of 18, is a criminal offence, even where the imagery is created, possessed, and distributed with the permission of the child depicted, or by the child themselves.

6. Grooming and exploitation

6.1 Grooming is defined as the situation whereby an adult builds a relationship, trust and emotional connection with a child with the intention of manipulating, exploiting and/or abusing them.

6.2 Staff will be aware that grooming often takes place online and that students who are being groomed are commonly unlikely to report this behaviour for many reasons, including the following:

- The student believes they are talking to another child, when they are actually talking to an adult masquerading as someone younger with the intention of gaining their trust to abuse them.
- The student does not want to admit to talking to someone they met on the internet for fear of judgement, feeling embarrassed, or a lack of understanding from their peers or adults in their life.
- The student may have been manipulated into feeling a sense of dependency on their groomer due to the groomer's attempts to isolate them from friends and family.
- Talking to someone secretly over the internet may make the student feel 'special', particularly if the person they are talking to is older.
- The student may have been manipulated into feeling a strong bond with their groomer and may have feelings of loyalty, admiration, or love, as well as fear, distress and confusion.

6.3 Due to the fact students are less likely to report grooming than other online offences, it is particularly important that staff understand the indicators of this type of abuse. The DSL will ensure that online safety training covers online abuse, the importance of looking for signs of grooming, and what the signs of online grooming are, including:

- Being secretive about how they are spending their time.
- Having an older boyfriend or girlfriend, usually one that does not attend the College and whom their close friends have not met.
- Having money or new possessions, e.g. clothes and technological devices, that they cannot or will not explain.

7. Child sexual exploitation (CSE) and child criminal exploitation (CCE)

7.1 Although CSE often involves physical sexual abuse or violence, online elements may be prevalent, e.g. sexual coercion and encouraging children to behave in sexually inappropriate ways through the internet. In some cases, a student may be groomed online to become involved in a wider network of exploitation, e.g. the production of child pornography or forced child prostitution and sexual trafficking.

7.2 CCE is a form of exploitation in which children are forced or manipulated into committing crimes for the benefit of their abuser, e.g. drug transporting, shoplifting and serious violence. While these crimes often take place in person, it is increasingly common for children to be groomed and manipulated into participating through the internet.

7.3 Where staff have any concerns about students with relation to CSE or CCE, they will bring these concerns to the DSL without delay.

8. Radicalisation

8.1 Radicalisation is the process by which a person comes to support terrorism and extremist ideologies associated with terrorist groups. This process can occur through direct recruitment, e.g. individuals in extremist groups identifying, targeting and contacting young people with the intention of involving them in terrorist activity, or by exposure to violent ideological propaganda. Children who are targets for radicalisation are likely to be groomed by extremists online to the extent that they believe the extremist has their best interests at heart, making them more likely to adopt the same radical ideology.

8.2 Staff members will be aware of the factors which can place certain students at increased vulnerability to radicalisation. Staff will be expected to exercise vigilance towards any students displaying indicators that they have been, or are being, radicalised.

8.3 Where staff have a concern about a student relating to radicalisation, they will report this to the DSL without delay.

9. Mental health

9.1 The internet, particularly social media, can be the root cause of a number of mental health issues in students, e.g. low self-esteem and suicidal ideation.

9.2 Staff will be aware that online activity both in and outside of College can have a substantial impact on a student's mental state, both positively and negatively. The DSL will ensure that training is available to help ensure that staff members understand popular social media sites and terminology, the ways in which social media and the internet in general can impact mental health, and the indicators that a student is suffering from challenges in their mental health.

10. Online hoaxes and harmful online challenges

10.1 For the purposes of this policy, an **"online hoax"** is defined as a deliberate lie designed to seem truthful, normally one that is intended to scaremonger or to distress individuals who come across it, spread on online social media platforms.

10.2 For the purposes of this policy, **"harmful online challenges"** refers to challenges that are targeted at young people and generally involve users recording themselves participating in an online challenge, distributing the video through social media channels and daring others to do the same. Although many online challenges are harmless, an online challenge becomes harmful when it could potentially put the participant at risk of harm, either directly as a result of partaking in the challenge itself or indirectly as a result of the distribution of the video online.

10.3 Where staff suspect there may be a harmful online challenge or online hoax circulating amongst students in the College, they will report this to the DSL immediately.

The DSL will conduct a case-by-case assessment for any harmful online content brought to their attention, establishing the scale and nature of the possible risk to students, and whether the risk is one that is localised to the College or the local area, or whether it extends more widely across the country. Where the harmful content is prevalent mainly in the local area, the DSL will consult with the LA about whether quick local action can prevent the hoax or challenge from spreading more widely.

10.4 Prior to deciding how to respond to a harmful online challenge or hoax, the DSL and the Head of School will decide whether each proposed response is:

- In line with any advice received from a known, reliable source, e.g. the UK Safer Internet Centre, when fact-checking the risk of online challenges or hoaxes.
- Careful to avoid needlessly scaring or distressing students.
- Not inadvertently encouraging students to view the hoax or challenge where they would not have otherwise come across it.
- Proportional to the actual or perceived risk.
- Supportive.

- In line with the Child Protection and Safeguarding Policy.

10.5 Where the DSL's assessment finds an online challenge to be putting students at risk of harm, e.g. it encourages children to participate in age-inappropriate activities that could increase safeguarding risks or become a child protection concern, they will ensure that the challenge is directly addressed to the relevant students.

The DSL and Head of School will only implement a college-wide approach to highlighting potential harms of a hoax or challenge when the risk of needlessly increasing students' exposure to the risk is considered and mitigated as far as possible.

11. Cyber-crime

11.1 Cyber-crime is criminal activity committed using computers and/or the internet. There are two key categories of cyber-crime:

- **Cyber-enabled** – these crimes can be carried out offline; however, are made easier and can be conducted at higher scales and speeds online, e.g. fraud, purchasing and selling of illegal drugs, and sexual abuse and exploitation.
- **Cyber-dependent** – these crimes can only be carried out online or by using a computer, e.g. making, supplying or obtaining malware, illegal hacking, and 'booting', which means overwhelming a network, computer or website with internet traffic to render it unavailable.

11.2 The College will factor into its approach to online safety the risk that students with a particular affinity or skill in technology may become involved, whether deliberately or inadvertently, in cyber-crime. Where there are any concerns about a student's use of technology and their intentions with regard to using their skill and affinity towards it, the DSL will consider a referral to the Cyber Choices programme, which aims to intervene where children are at risk of committing cyber-crime and divert them to a more positive use of their skills and interests.

11.3 The DSL and Head of School will ensure that students are taught, throughout the curriculum, how to use technology safely, responsibly and lawfully, and will ensure that students cannot access sites or areas of the internet that may encourage them to stray from lawful use of technology.

12. Online safety training for staff

12.1 The DSL ensures that all safeguarding training given to staff includes elements of online safety, including how the internet can facilitate abuse and exploitation. All staff will be made aware that students are at risk of abuse, by their peers and by adults, online as well as in person, and that, often, abuse will take place concurrently via online channels and in daily life.

13. Use of technology in the classroom

13.1 A wide range of technology is used during lessons, including the following:

- Computers
- Laptops
- Tablets
- Cameras

13.2 Prior to using any websites, tools, apps or other online platforms in learning sessions or recommending that students use these platforms at home, staff will always review and evaluate the resource.

13.3 Students are supervised when using online materials during lesson time – this supervision is suitable to their age and ability.

14. Use of smart technology

14.1 While the College recognises that the use of smart technology can have educational benefits, there are also a variety of associated risks which the school will ensure it manages. Students will be educated on the acceptable and appropriate use of personal devices and will use technology.

14.2 The school recognises that students require education about inappropriate use of smart technology including:

- Using mobile and smart technology to sexually harass, bully, troll or intimidate peers.
- Sharing indecent images, both consensually and non-consensually.
- Viewing and sharing pornography and other harmful content.

14.3 The College will seek to ensure that it is kept up to date with the latest devices, platforms, apps, trends and related threats.

The College will consider the 4C's (content, contact, conduct and commerce) when educating students about the risks involved with the inappropriate use of smart technology and enforcing the appropriate disciplinary measures.

15. Educating parents

15.1 The College works in partnership with parents to ensure students stay safe online at College and at home. Parents are provided with information about the College's approach to online safety and a copy of the Acceptable Use Agreement which they are encouraged to go through with their child to ensure their child understands the document and the implications of not following it.

15.2 Parents will be made aware of the various ways in which their children may be at risk online, including, but not limited to:

- Child sexual abuse, including grooming.
- Exposure to radicalising content.
- Sharing of indecent imagery of pupils, e.g. sexting.
- Cyberbullying.
- Exposure to age-inappropriate content, e.g. pornography.
- Exposure to harmful content, e.g. content that encourages self-destructive behaviour.

16. Internet access

16.1 Students, staff and other members of the College community are only granted access to the College's internet network once they have read and signed the Acceptable Use Agreement. A record is kept of users who have been granted internet access in the College office.

16.2 All members of the College community are encouraged to use the College's internet network, instead of 3G, 4G and 5G networks, as the network has appropriate filtering and monitoring to ensure individuals are using the internet appropriately.

17. Network security

17.1 Technical security features, such as anti-virus software, are kept up-to-date and managed by an external IT company.

17.2 Firewalls are switched on at all times.

17.3 Staff and students are advised not to download unapproved software or open unfamiliar email attachments, and are expected to report all malware and virus attacks to a member of staff.

17.4 All members of staff have their own unique usernames and private passwords to access the school's systems. Students are provided with their own unique username and private passwords. Staff members and students are responsible for keeping their passwords private.

17.5 Users are required to lock access to devices and systems when they are not in use.
Full details of the College's network security measures can be found in the Data and Cyber-security Breach Prevention and Management Plan.

18. Emails

18.1 Access to and the use of emails is managed in line with the GDPR Policy and the Acceptable Use Agreement.
18.2 Staff are given approved College email accounts and are only able to use these accounts at College and when doing College-related work outside of College hours. Prior to being authorised to use the email system, staff must agree to and sign the Acceptable Use Agreement.
18.3 Staff members are required to block spam and junk mail, and report the matter to the member of staff responsible for ICT. The College's monitoring system can detect inappropriate links, malware and profanity within emails – staff are made aware of this. Chain letters, spam and all other emails from unknown sources are deleted without being opened.

19. Social networking - Personal use

19.1 Access to social networking sites is filtered as appropriate. Staff are not permitted to use social media for personal use during College hours.
19.2 Staff members are advised that their conduct on social media can have an impact on their role and reputation within the College.
19.3 Staff are not permitted to communicate with students or parents over social networking sites and are reminded to alter their privacy settings to ensure students and parents are not able to contact them on social media. Where staff have an existing personal relationship with a parent or student, and thus are connected with them on social media, they will disclose this to the DSL and Head of School and will ensure that their social media conduct relating to that parent is appropriate for their position in the school.
19.4 Students are taught how to use social media safely and responsibly through the online safety curriculum.
19.5 Concerns regarding the online conduct of any member of the College community on social media are reported to the DSL and managed in accordance with the relevant policy.

20. The College website

20.1 The Executive Headteacher and Head of School are responsible for the overall content of the College website – they will ensure the content is appropriate, accurate, up-to-date and meets government requirements.
20.2 The website complies with guidelines for publications including accessibility, data protection, respect for intellectual property rights, privacy policies and copyright law. Personal information relating to staff and students is not published on the website. Images and videos are only posted on the website if the relevant permissions have been sought.

21. Use of devices

21.1 College-owned devices

21.1.1 Staff members are issued with the following devices to assist with their work:

- Mobile phone
- Laptop – if required

21.1.2 Students are provided with college-owned devices as necessary to assist in the delivery of the curriculum, e.g. laptops to use during lessons or for remote learning.
21.1.3 College-owned devices are used in accordance with the Acceptable User Agreement.
21.1.4 All College-owned devices are password protected.

21.1.5 No software, apps or other programmes can be downloaded onto a device without authorisation from the DSL.

21.2 Personal devices

21.2.1 Any personal electronic device that is brought into school is the responsibility of the user.

21.2.2 Staff members are not permitted to use their personal devices to take photos or videos of students.

21.2.3 Staff members are to report concerns about their colleagues' use of personal devices on the College premises in line with the Allegations of Abuse Against Staff Policy. If a member of staff is thought to have illegal content saved or stored on a personal device, or to have committed an offence using a personal device, the Executive Headteacher or Head of School will inform the police.

21.2.4 If a staff member reasonably believes a student's personal device has been used to commit an offence or may provide evidence relating to an offence, the device will be handed to the police.

22. Remote learning

22.1 The College will risk assess the technology used for remote learning prior to use and ensure that there are no privacy issues or scope for inappropriate use. The College will consult with parents prior to the period of remote learning about what methods of delivering remote teaching are most suitable – alternate arrangements will be made where necessary.

22.2 During the period of remote learning, the College will maintain regular contact with parents to:

- Reinforce the importance of children staying safe online.
- Ensure parents are aware of what their children are being asked to do, e.g. sites they have been asked to use and staff they will interact with.
- Encourage them to set age-appropriate parental controls on devices and internet filters to block malicious websites.
- Direct parents to useful resources to help them keep their children safe online.

22.3 The College will not be responsible for providing access to the internet off the College premises.