Creative
Education
Trust

Online Safety Policy

Policy name
This policy may be referred to in other policies as e-safety, for the purposes of this policy the terms "online safety" and "e-safety" should be treated as synonymous.

Policy Owner	**Director of IT and EdTech**
Approved by	**CEO and Safeguarding Committee**
Last reviewed on	**December 2025**
Next review date	**December 2027**

CONTENTS

PRINCIPLES

1) Creative Education Trust (CET) is committed to providing a safe and secure environment for students, staff and visitors and promoting a climate where students and adults feel confident about sharing any concerns that they may have about their own safety or the wellbeing of others.

2) This policy aims to educate the whole school community about their access to and use of technology and to establish effective mechanisms to identify, intervene and escalate incidents where appropriate.

3) CET identifies that the issues classified within online safety are considerable, but can be broadly categorised into four areas of risk:

   a) **CONTENT:** being exposed to illegal, inappropriate or harmful material
   b) **CONTACT:** being subjected to harmful online interaction with other users
   c) **CONDUCT:** personal online behaviour that increases the likelihood of, or causes, harm
   d) **COMMERCE**: risks such as online gambling, inappropriate advertising, phishing and or financial scams

4) This policy aims to promote a culture of safety, equality and protection in school.

5) This policy should be read and implemented in conjunction with the following policies:
   a) Anti-Bullying Policy
   b) Artificial Intelligence (AI) Policy
   c) Behaviour for Learning Policy
   d) Child Protection Policy
   e) Data Protection Policy
   f) Staff Code of Conduct
   g) Whistleblowing Policy

6) The policy applies to all members of the school community, including staff and volunteers, students, parents and visitors, who have access to the school's technology whether on or off school premises, or otherwise use technology in a way which affects the welfare of other students or any member of the school community or where the culture or reputation of the school is put at risk.

REGULATORY AND GUIDANCE FRAMEWORK

7) This policy aligns with relevant UK legislation and statutory guidance, including Keeping Children Safe in Education (DfE, 2025), the Online Safety Act 2023, the Data Protection Act 2018 (UK GDPR), and the Equality Act 2010.

PUBLICATION AND AVAILABILITY OF THIS POLICY

8) This policy is published on the school website. Printed or accessible versions are available on request.

DEFINITIONS

9) All references to school include the school and CET.

10) In considering the scope of the school's online safety strategy, the school will take a wide and purposive approach to considering what falls within the meaning of technology, networks and devices used for viewing or exchanging information (collectively referred to in this policy as technology).

11) All references to parent or parents includes any individual with parental responsibility or care for a student, whether biological, adoptive, or acting as a carer or legal guardian.

SCOPE AND RESPONSIBILITIES

12) This policy applies to **ALL STAFF** including the governing body, teachers, support staff, external contractors, visitors, volunteers and other individuals who work for, or provide services on behalf of the school (collectively referred to as 'staff' in this policy) as well as students and parents/carers.

13) This policy applies to all use of the internet and digital technology by members of the school community. It covers activity on school systems and devices, as well as on personal devices when:
    a) they are connected to or used to access school networks, systems, or data; or
    b) their use impacts the safety or wellbeing of students or staff or affects the reputation of the school (for example, online bullying, harassment or sharing harmful content).

14) The **PRINCIPAL/HEADTEACHER** is responsible for implementing this policy, publishing it on the school's website and ensuring that all staff at the school are aware of and comply with it.

15) The school's **DESIGNATED SAFEGUARDING LEAD** (DSL) will take lead responsibility for online safety and understanding the filtering and monitoring systems and processes in place.

16) In addition to the DSL, the school **LEADERSHIP TEAM AND OTHER RELEVANT STAFF** will also understand how to manage and act on concerns arising from filtering and monitoring systems.

17) The school's **ONLINE SAFETY LEAD** acts as the school's main point of contact for all online safety matters. They are responsible for coordinating online safety across the school, including:
    a) monitoring safeguarding alerts from filtering and monitoring systems, recording and escalating concerns appropriately.

b) liaising with the Designated Safeguarding Lead (DSL), CET Safeguarding and IT Directorates to ensure effective and compliant filtering and monitoring.
c) maintaining accurate records of online safety incidents on CPOMS.
d) leading regular reviews of online safety arrangements.
e) overseeing staff training and induction and ensuring online safety is embedded in the curriculum.
f) promoting awareness among students, staff and parents through regular communication.
g) attending Trust training and briefings to maintain current knowledge of legislation, systems and best practice.

18) **ALL STAFF** members:
a) will know who the school's Online Safety Lead is.
b) will read and adhere to this policy and Acceptable Use appendices.
c) will take responsibility for the security of school systems and the data they use or have access to.
d) will model good practice when using technology and maintain a professional level of conduct in their personal use of technology, both on and offsite.
e) embed online safety education in curriculum delivery, wherever possible.
f) will have an awareness of a range of online safety issues and how they may be experienced by the children in their care.
g) will identify online safety concerns and take appropriate action by following the school's safeguarding policies and procedures.
h) will know when and how to escalate online safety issues, including signposting to appropriate support, internally and externally.

19) The school's **IT SUPPORT TEAM**:
a) will provide technical support and perspective to the Online Safety Lead and leadership team.
b) will implement appropriate security measures (including password policies and encryption) to ensure that the school's IT infrastructure/systems are secure and not open to misuse or malicious attack, whilst allowing learning opportunities to be maximised.
c) will ensure that the school's filtering policy is applied and updated on a regular basis
d) will report any filtering breaches to the Online Safety Lead and leadership team, as well as, the school's web filtering provider or other services, as appropriate.

20) **STUDENTS** (at a level appropriate to their individual age, ability and vulnerabilities):
a) will read and adhere to the Acceptable Use Policy.
b) will engage in age-appropriate online safety education opportunities.
c) will respect the feelings and rights of others both on and offline.
d) will take responsibility for keeping themselves and others safe online.
e) will seek help from a trusted adult, if they have a concern related to their online activities and will support others that may be experiencing online safety issues.

21) **PARENTS** are encouraged to:
  a) read this policy and Acceptable Use appendices and encourage their children to adhere to it.
  b) support the school in the implementation of this policy by discussing online safety issues with their children and reinforcing safe online behaviours at home.
  c) role model safe and appropriate use of technology and social media and will endeavour to understand the ways in which they are using the internet, social media and their mobile devices to promote responsible behaviour.
  d) remain alert to changes in their child's behaviour that may suggest they are at risk online.
  e) seek help and support from the school, or other appropriate agencies, if they or their child have online safety concerns.
  f) use school systems, such as learning platforms and other network resources, safely and appropriately.
  g) keep up to date with the risks and opportunities of new and emerging technologies.

Where appropriate school leaders will always signpost parents to useful resources about online safety.

INDUCTION AND TRAINING

22) As part of their induction, all new staff will be provided with a copy of this policy.

23) At induction, all new staff will also be introduced to the Online Safety Lead who will explain their role and provide them with online safety training so that they are aware of how to deal appropriately with incidents involving the use of technology when they occur. This includes being able to recognise the additional risk that children with SEN and Disabilities (SEND) face online, so that staff are confident they have the capability to support SEND children to stay safe online.

24) Where safeguarding incidents involve youth produced sexual imagery, staff will follow the principles laid out in the school's Child Protection policy, and Keeping Children Safe in Education (2025).

25) All staff will receive regular online safety updates as part of their safeguarding and child protection training. This will include emerging risks such as AI misuse and deepfakes, as well as specific safeguarding issues including the sharing of nudes or semi-nude images, cyberbullying, radicalisation, and harmful online challenges or hoaxes.

26) All members of the school community will be made aware of the school's expectations regarding safe and appropriate behaviour online and the importance of not posting any content, comments, images or videos which could cause harm, distress or offence to members of the community. This is clearly outlined in the Acceptable Use appendices in this policy and highlighted through a variety of education and training approaches.

EDUCATION AND THE CURRICULUM

27) Students will be taught about safeguarding, including online safety, through teaching and learning opportunities within the curriculum. In addition, these messages are reinforced as part of assemblies, tutorial or pastoral activities.

28) Students will be taught about the importance of safe and responsible use of technology, including the internet, social media and mobile electronic devices. Those parts of the curriculum that deal with the safe use of technology are reviewed on a regular basis to ensure their relevance.

29) Students will be taught to think critically about the online content they encounter, including how to identify and respond to misinformation, disinformation, and conspiracy theories, whether human or AI-generated. They will learn to verify information for accuracy and to credit reliable sources appropriately.

30) Students will be taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet.

31) Students will be taught about the risks associated with using the technology and how to protect themselves and their peers from potential risks.

32) Students will be taught how to recognise suspicious, manipulative, dishonest, bullying or extremist behaviour.

33) Students will be taught what cyberbullying is, its impact on victims, and the importance of showing respect for others' online identities. They will also learn how to report incidents that make them or others feel unsafe or uncomfortable, and how the school responds to such behaviour.

34) Students will be taught the consequences of negative online behaviour.

35) Students will be helped to understand the need for the Acceptable Use appendices in this policy and encouraged to adopt safe and responsible use both within and outside school. Students will be reminded of the importance of the Acceptable Use appendices in this policy on a regular basis.

36) In planned lessons involving internet use, students will be directed to age-appropriate, pre-checked websites, and staff will follow agreed procedures if unsuitable material is accessed or discovered.

37) When students are permitted to search the internet independently, staff will supervise their activity appropriately and provide support where needed. Additional care will be taken to assist students with SEND who may require extra guidance to stay safe online.

38) It is accepted that from time to time, for good educational reasons, students may need to

research topics (e.g. racism, drugs, discrimination) that would normally result in internet searches being blocked. In such a situation, staff can request that the IT team temporarily remove specific websites from the filtered list for the period of study. Any request to do so should be raised via the CET Service Desk, with clear reasons for the need.

MANAGING THE IT INFRASTRUCTURE

39) The school takes appropriate steps to ensure the security of its information systems, including:
   a) virus protection being updated regularly so that, as far as possible, the school's network and technology is not open to misuse or malicious attack.
   b) encryption of personal data sent over the Internet, taken off site or accessed via appropriate secure remote access systems.
   c) not using portable media without specific permission.
   d) not downloading unapproved software to work devices or opening unfamiliar email attachments or links.
   e) regularly monitoring the school's network and technology to ensure that misuse or attempted misuse can be identified and reported to the appropriate person for investigation.
   f) ensuring that the risk of users being able to circumvent the safeguards put in place by the school are minimised.
   g) the appropriate use of user logins and passwords to access the school network and technology to ensure that users ae properly authenticated and authorised:
      - specific user logins and passwords will be enforced for all but the youngest users (Early Years Foundation Stage children).
   h) all users must log off or lock their screens/devices if systems are unattended.
   i) aligning with the DfE Cyber Security Standards for Schools and Colleges and utilising National Cyber Security Centre (NCSC) training and guidance to strengthen cyber resilience.

40) All staff must take appropriate steps to ensure the security of the school's information systems, including:
   a) setting up and utilising multi-factor authentication when accessing school systems remotely to reduce the risk of unauthorised access.
   b) completing annual cyber security training.

PASSWORD POLICY

41) Members of staff will have their own unique username and passwords to access school systems; members of staff are responsible for keeping their password private.
42) Members of staff must not record passwords or encryption keys in unprotected files or unsecured locations (such as on post-it notes).

43) Members of staff must use different passwords for different accounts to reduce the risk of compromise. Passwords used for school systems must not be reused for any personal or non-school accounts.

44) From Year 1, students will normally be provided with their own unique login credentials to access school systems. Students are responsible for keeping their login details secure and private.

45) CET require all users to:
   a) use strong passwords for access into school systems.
   b) change passwords whenever there is any indication of possible system or password compromise.
   c) always keep their password private; users must not share it with others or leave it where others can find it.
   d) inform the IT team immediately if they are aware of a breach of security with their password or account.

SCHOOL WEBSITE

46) The school will ensure that information posted on the school website meets the requirements as identified by the Department for Education (DfE).

47) The school will ensure that the school website complies with guidelines for publications including accessibility, data protection, respect for intellectual property rights, privacy policies and copyright.

48) Staff personal information will not be published on the school's website unless required for their professional role. In such cases, only names and work contact details will be shared. The website may also include names, photographs, and success stories of staff and students, but these will only be published where appropriate consent has been obtained in line with the school's data protection policies.

49) The administrator account for the school website will be secured with an appropriately strong password.

50) The school will post appropriate information about safeguarding, including online safety, on the school website for members of the community.

EMAIL

51) Access to school email systems will always take place in accordance with data protection legislation and in line with other policies, including the Data Protection Policy and the Acceptable Use appendices in this policy.
   a) The forwarding of any chain messages/emails is not permitted. Spam or junk mail will be blocked and reported to the email provider.
   b) Attachments or links must not be opened in emails where the sender is unknown or from emails or websites that look suspicious. If the user is unsure, they must contact the IT team.
   c) Any electronic communication which contains sensitive or personal information will only be sent using secure and encrypted email.
   d) School email addresses and other official contact details must not be used to register for personal accounts, including social media.

52) The use of school Office 365 accounts on personal smartphones/tablets is permitted provided the following conditions are met:
    a) the device has been enrolled into the school's device management platform to ensure security compliance.
    b) the device is protected by a PIN/Passcode.
    c) the device has remote wipe capability.
    d) IT Support are informed immediately if the device is lost or stolen.

53) The use of personal email addresses by staff for any official school business is not permitted.
    a) All members of staff are provided with a specific school email address, to use for all official communication.
    b) Students will use school-provided email accounts for educational purposes.

FILTERING AND MONITORING

54) The school, through the DSL, Online Safety Lead and Regional IT Manager, will ensure that appropriate filtering and monitoring is in place and that reasonable precautions are taken to restrict access to unsuitable material.

55) All users will be informed that use of school systems can be monitored and that all monitoring will be in line with data protection, human rights and privacy legislation.

56) The school will have age-appropriate filtering and monitoring systems in place, to limit children's exposure to online risks:
    a) Illegal content, e.g. child sexual abuse images, will be filtered by the filtering provider through active employment of the Internet Watch Foundation CAIC list.
    b) Sites that fall into categories such as pornography, racial hatred, extremism, self-harm, violence, drugs / substance abuse, hacking, piracy, gaming and sites of an illegal nature will all be blocked by the filtering system.
    c) Unapproved AI tools and chatbots will be blocked by the filtering system.
    d) Content lists will be updated and Internet use will be logged and monitored regularly.
    e) The filtering system will provide appropriate filtering levels for different ages and groups of users such as staff, primary school and secondary school students.
    f) The filtering and monitoring systems will be configured to send automated safeguarding alerts and reports to the Online Safety Lead to help identify students who are likely to be at risk based on their usage of school devices and Internet.
    g) The Online Safety Lead, where that individual is not also the Designated Safeguarding Lead, will immediately advise the latter of any concern that emerges.

57) While the school takes all reasonable precautions to prevent access to unsuitable or offensive material, the global and connected nature of the internet means that no system can guarantee 100% protection.

58) All users must not view, retrieve, download or share any offensive material. Offensive

material includes, but is not limited to, content that is abusive, racist, considered to be of an extreme or terrorist related nature, sexist, homophobic, any form of bullying, pornographic, defamatory or criminal activity.

59) Use of technology in this way is a serious breach of discipline and may constitute a criminal offence. Students must tell a member of staff immediately if they have accidentally read, downloaded or have been sent any offensive material or material that is inappropriate, including personal information about someone else.

GENERATIVE AI

60) This section should be read in conjunction with the CET Artificial Intelligence (AI) Policy.

61) Only generative AI tools that have been approved by the Trust may be used. These tools should align with the DfE's Generative AI: Product Safety Expectations and provide:
   a) robust filtering that prevents access to harmful or inappropriate content and covers text, images, audio and other outputs, with settings adjusted by age and risk;
   b) monitoring and moderation that logs all usage, produces real-time alerts and generates reports that non-expert staff can interpret;
   c) security, data-protection and privacy controls consistent with the **CET AI Policy**.

62) Students may only access generative AI when directed by a member of staff as part of a curriculum-linked activity; they must not bypass filters, use personal AI accounts or share personal data in prompts. Where AI is used, students are taught to treat outputs critically, cross-check information for accuracy and bias, and cite sources.

63) Staff may only use generative AI through approved accounts with appropriate enterprise safeguards. Personal or publicly available (open) AI accounts must not be used for work purposes. Staff remain responsible for the content of any AI output used in teaching, assessment or other administrative work, such as communication, and must complete relevant training before using AI tools.

64) Concerns relating to AI-generated content or student behaviour involving AI that raise safeguarding issues must be reported to the Online Safety Lead or DSL. The Online Safety Lead will investigate, liaise with the Central IT Team where required, and adjust filtering or monitoring settings as necessary in line with the CET AI Policy.

65) The school will ensure that students are taught about AI literacy (how generative AI works, its limitations, the risk of mis/disinformation and ethical considerations) and will reinforce the importance of critical thinking and human judgement when interacting with AI tools.

DATA SECURITY

66) Personal data will be collected, stored and processed in accordance with The Data Protection Act 2018.

67) Staff must ensure that they:
   a) at all times take care to ensure the safe keeping of personal data, minimising the risk of its loss or misuse.
   b) access and use personal data only on secure, password-protected devices. Computers or devices must be locked when unattended and users must log off fully at the end of each session involving personal data.
   c) transfer data using encryption and secure password protected devices.
   d) follow the software service request process on the CET Service Desk prior to signing up to any new software or online systems (including any free of charge services).
   e) do not input the names of students, staff, members of the school community, or any other sensitive information into an AI tool unless it has been approved for secure use by the Trust.
   f) comply with the CET Data Protection Policy.

68) Staff use of personal external storage devices such as USB memory sticks and portable hard drives is **PROHIBITED**. Use of an encrypted school-supplied external storage device is permitted where a staff member has a requirement to utilise one for work purposes and the usual secure school storage locations such as OneDrive Cloud storage are not feasible. The external storage device remains the property of the school and must be returned at the end of employment.

69) When personal data is stored on any portable computer system, memory stick or any other removable media:
   a) the data must be encrypted and password protected with a strong password.
   b) the device must be password protected.
   c) the device must offer approved virus and malware checking software.
   d) the data must be securely deleted from the device, once it has been transferred or its use is complete.

CLASSROOM TECHNOLOGY

70) The school uses a wide range of technology. This includes:
   a) computers, laptops, tablets and other digital devices.
   b) internet which may include search engines and educational websites.
   c) school learning tools/portals.
   d) email.
   e) digital cameras, web cams and video cameras.

71) All school-owned devices will be used in accordance with the requirements contained in the Acceptable Use appendices in this policy and with appropriate safety and security measures in place.

72) Staff will take reasonable steps to check the suitability of websites, tools and apps before use in the classroom or recommending for use at home.

73) The school will use age-appropriate search tools for students, such as Google Safe Search.

74) The school will ensure that the use of internet-derived materials, by staff and students, complies with copyright law and acknowledge the source of information.

75) Supervision of students will be appropriate to their age and ability:
   a) Early Years Foundation Stage and Key Stage 1:
      - Students' access to the internet will be by adult demonstration, with occasional directly supervised access to specific and approved on-line materials, which supports the learning outcomes planned for the students' age and ability.
   b) Key Stage 2:
      - Students will use age-appropriate search engines and online tools.
      - Children will be directed by the teacher to online materials and resources which support the learning outcomes planned for the student's age and ability.
   c) Key Stage 3, 4 and 5:
      - Students will be appropriately supervised when using technology, according to their ability and understanding.

VIDEO CONFERENCING TECHNOLOGY AND REMOTE LEARNING

76) Online meeting invitation links must not be shared with or accessed by others unless permission has been granted by the meeting organiser.

77) The use of on-line learning tools and systems must be in line with privacy and data protection requirements.

78) When delivering on-line lessons, the following must be adhered to.
   a) Normally, no 1:1 activity with students, groups only. When 1:1 contact is required, such as for well-being calls, careers interviews or post-16 tutorials, these calls may be made by phone, in line with the Code of Conduct, or via an approved online platform such as Teams. Any 1:1 online calls and meetings should normally be recorded unless the DSL has approved an alternative safeguarding arrangement.
   b) Staff must wear appropriate clothing, and anyone else in the household who may appear must be clothed.
   c) Any computers used should be in appropriate areas, for example, not in bedrooms; and the background should be blurred.
   d) Language must be professional and appropriate, including any family members in the background.
   e) Staff must only use platforms provided by the school to communicate with students.
   f) Staff must follow Trust guidance when setting up on-line lessons to ensure that appropriate safeguarding settings are in place to prevent unauthorised use and access to on-line lessons.

USE OF PERSONAL DEVICES AND MOBILE PHONES

79) Mobile phones brought into school are entirely at the staff member's, student's, parent's or visitor's own risk. The school accepts no responsibility for the loss, theft or damage of any mobile phone or personal device brought into School.

STUDENTS

80) Students must not use personal mobile data (for example, hotspotting or tethering) to bypass the school's filtering or monitoring systems. This applies to all smart devices.

81) Electronic devices may be confiscated and searched in appropriate circumstances. See the school's Behaviour for Learning Policy on the searching of electronic devices.

82) Students should be aware that the use of electronic devices of any kind to bully, harass, intimidate or attempt to radicalise others will not be tolerated and is likely to constitute a serious breach of discipline, whether or not the student is in the care of the school at the time of such use. Appropriate disciplinary action will be taken where the school becomes aware of such use (see the school's Anti-Bullying Policy and Behaviour for Learning Policy). The school's Child Protection Policy and procedures will be followed in appropriate circumstances (see the school's Child Protection Policy and procedures).

83) Students will be taught that sending unsolicited sexual images (cyberflashing) or creating or sharing intimate images without consent (including deepfakes) is illegal and prohibited. If students (or staff) encounter such content they must report it.

STAFF

84) The use of personal mobile phones or cameras by staff is not permitted at any time when students are present. The only exception to this is the use of a mobile phone to communicate during an emergency situation.

85) Members of staff will ensure that use of personal phones and devices takes place in accordance with the law, as well as, relevant school policy and procedures, such as the CET Child Protection Policy, CET Data Protection Policy and the Acceptable Use appendices in this policy.

86) Staff are advised to:
   a) Keep mobile phones and personal devices in a safe and secure place during lesson time.
   b) Keep mobile phones and personal devices switched off or switched to 'silent' mode during lesson times.
   c) Ensure that Bluetooth or other forms of communication (such as 'airdrop') are hidden or disabled during lesson times.
   d) Ensure that any content brought onto site via mobile phones and personal devices are compatible with their professional role and expectations.

87) Members of staff are not permitted to use their own personal phones for contacting students or parents and carers, unless explicit written permission has been provided by the Principal/Headteacher in exceptional circumstances.

88) Staff will not use personal devices, such as: mobile phones, tablets or cameras:
    a) to take photos or videos of students and will only use work-provided equipment for this purpose
    b) directly with students and will only use work-provided equipment during lessons/educational activities.

89) Where staff members are required to use a mobile phone for school duties, for instance in case of emergency during off-site activities, or for contacting students or parents/carers, then a school phone will be provided and used. In an emergency where a staff member doesn't have access to a school-owned device, they should use their own device and hide (by inputting 141) their own mobile number for confidentiality purposes.

DIGITAL IMAGES AND VIDEOS

90) The school will gain parental/carer permission for use of digital photographs or video involving their child.

91) The school will avoid publishing the full names of students alongside their photographs or in the credits of school-produced video materials. Full names may only be used where appropriate consent has been obtained and where it is considered necessary and safe to do so, in line with the school's data protection policies.

STUDENTS

92) Students will be taught that posting photos or videos on social media or websites (such as YouTube) that could, in the reasonable opinion of the Principal or Headteacher, constitute a criminal offence or bring the school into disrepute, is a serious breach of discipline and may result in formal disciplinary action.

93) Students will be taught to take great care when sharing personal photos or information online and to use privacy settings to keep personal content secure and not publicly accessible.

94) Students will be taught not to post images or videos of others without consent and to understand the risks of sharing identifying details (such as file names, location data, or addresses). They will also learn how to protect their data and what to do if they experience bullying or abuse as a result of online content.

STUDENTS AND STAFF

95) *SEXTING AND CYBERFLASHING*
    a) Students are taught that sharing nudes or semi-nude images (sexting) and sending unsolicited sexual images (cyberflashing) are illegal and harmful under the Online Safety Act 2023.
    b) Lessons highlight the risks of exploitation, blackmail, and emotional harm, and how to report concerns to staff.
    c) Staff must record and escalate all incidents involving intimate-image abuse (including deepfakes) as safeguarding concerns.

96) *UPSKIRTING*
   a) Upskirting, taking or attempting to take images under clothing without consent, is a criminal offence.
   b) The school treats all incidents as both a disciplinary and safeguarding matter in line with the Child Protection Policy.
   c) Students are advised to speak to a member of staff immediately if they believe they have been affected.

97) DEEPFAKES
   a) Deepfakes are digitally altered or created images, videos, or audio that falsely depict an individual. When used to create intimate or explicit content, this is intimate image abuse and a criminal offence under the Online Safety Act 2023.
   b) Creation, sharing, or threats to share deepfakes are strictly prohibited.
   c) Staff must record and escalate all incidents involving deepfakes or other intimate-image abuse as safeguarding concerns.

SOCIAL MEDIA

98) The expectations regarding safe and responsible use of social media applies to all academy counsellors, members and trustees, staff, external contractors, visitors, volunteers and other individuals who work for, or provide services on behalf of, the school or CET.

99) The school will control student and staff access to social media whilst using school provided devices and systems on site.
   a) The use of social media during school hours for personal use is not permitted.
   b) The school blocks/filters access to social networking sites unless approved by the Principal/Headteacher for a specific purpose such as to enable a member of staff to perform their duties.

STAFF PERSONAL USE OF SOCIAL MEDIA

REPUTATION

100) Safe and professional behaviour will be outlined for all members of staff (including volunteers) as part of the Acceptable Use appendices set out at the end of this policy.

101) All members of staff are advised that their online conduct on social media can have an impact on their role and reputation within school. Civil, legal or disciplinary action may be taken if they are found to bring the profession or institution into disrepute, or if something is felt to have undermined confidence in their professional abilities.

102) All members of staff are advised to safeguard themselves and their privacy when using social media sites. Advice will be provided to staff via staff training and by sharing appropriate guidance and resources. This will include (but is not limited to):
   a) setting the privacy levels of their personal sites as strictly as they can.
   b) being aware of location sharing services.
   c) opting out of public listings on social networking sites.

d) logging out of accounts after use.
e) keeping passwords safe and confidential.
f) ensuring staff do not represent their personal views as that of the school.

103) Members of staff are encouraged not to identify themselves as employees of the school on their personal social networking accounts. This is to prevent information on these sites from being linked with the school and also to safeguard the privacy of staff members. The Trust recognises that some staff will use social media to promote their professional profile. Where this is the case staff must ensure that their online conduct aligns with what would be reasonably expected of an adult working at the school, the Code of Conduct and this policy.

104) All members of staff are encouraged to carefully consider the information, including text and images, they share and post online and to ensure that their social media use is compatible with their professional role and is in accordance with school policies and the wider professional and legal framework. Information and content that staff members have access to as part of their employment, including photos and personal information about students and their family members or colleagues will not be shared or discussed on social media sites.

105) Members of staff will notify a member of the school leadership team immediately if they consider that any content shared on social media sites conflicts with their role in the school.

106) Members of staff must take all reasonable steps to maintain appropriate separation between their professional and personal lives, ensuring that their behaviour, communications, and use of technology do not compromise their professional integrity or the reputation of the school.

COMMUNICATING WITH STUDENTS, PARENTS AND CARERS

107) All members of staff are advised not to communicate with or add as ‘friends’ any current or past students or current or past students’ family members via any personal social media sites, applications or profiles.
a) Any pre-existing relationships or exceptions that may compromise this will be discussed with the DSL and/or the Principal/Headteacher.
b) If ongoing contact with students is required once they have left the school, members of staff will be expected to use official school-provided communication tools.

108) Any communication from students and parents/carers received on personal social media accounts will be reported to the Principal/Headteacher.

STUDENTS’ PERSONAL USE OF SOCIAL MEDIA

109) Safe and appropriate use of social media will be taught to students as part of an embedded and progressive education approach, via age-appropriate sites and resources.

110) Any concerns regarding students' use of social media, both at home and at school, will be dealt with in accordance with existing school policies including the Anti-Bullying Policy, Behaviour for Learning Policy and the Child Protection Policy. Concerns will also be raised with parents/carers as appropriate, particularly when concerning under-age use of social media sites or tools.

111) Students will be advised:
a) to consider the benefits and risks of sharing personal details on social media sites which could identify them and/or their location. Examples would include real/full name, address, mobile or landline phone numbers, school attended, other social media contact details, email addresses, full names of friends/family, specific interests and clubs.
b) to only approve and invite known friends on social media sites and to deny access to others by making profiles private/protected.
c) not to meet any online friends without a parent/carer or other responsible adult's permission and only when a trusted adult is present.
d) to use safe passwords.
e) to use social media sites which are appropriate for their age and abilities.
f) how to block and report unwanted communications and report concerns both within school and externally.

OFFICIAL USE OF SOCIAL MEDIA

112) The official use of social media sites, by the school, only takes place with clear educational or community engagement objectives, with specific intended outcomes. The following must be adhered to.
a) The official use of social media as a communication tool has been approved by the Principal/Headteacher.
b) Leadership staff have access to account information and login details for the social media accounts, in case of emergency, such as staff absence.
c) The number of social media accounts per platform should be minimised to ensure control of the content being submitted and to reduce the risk of unauthorised access.
d) Access to school social media accounts and pages must be disabled when staff have left the school or no longer have responsibility for social media at the school.

113) Official school social media channels must be set up as distinct and dedicated social media sites or accounts for educational or engagement purposes only in line with the following conditions.
a) Staff use school-provided email addresses to register for and manage any official school social media channels.
b) Official social media sites are suitably protected and, where possible, run and/or linked to/from the school website.
c) Public communications on behalf of the school will, where appropriate and possible, be read and agreed by at least one other colleague.

114) Official social media use will be conducted in line with existing policies, including:

Anti-Bullying Policy, Child Protection Policy and Data Protection Policy.

a) All communication on official social media platforms will be clear, transparent and open to scrutiny.

115) The school will ensure that any official social media use does not exclude members of the community who are unable or unwilling to use social media channels.

STAFF EXPECTATIONS

116) Members of staff who follow and/or like the school social media channels are advised to use dedicated professional accounts, where possible, to avoid blurring professional boundaries.

117) If members of staff are participating in on-line social media activity as part of their capacity as an employee of the school, they will:

a) be professional at all times and aware that they are an ambassador for the school.
b) disclose their official role and/or position, but make it clear that they do not necessarily speak on behalf of the school.
c) be responsible, credible, fair and honest at all times and consider how the information being published could be perceived or shared.
d) always act within the legal frameworks they would adhere to within the workplace, including: libel, defamation, confidentiality, copyright, data protection and equalities laws.
e) ensure that they have appropriate written consent before posting images on the official social media channel.
f) not disclose information, make commitments or engage in activities on behalf of the school unless they are authorised to do so.
g) not engage with any direct or private messaging with current, or past, students, parents and carers.
h) inform their line manager, the DSL and/or the Principal/Headteacher of any concerns, such as criticism, inappropriate content or contact from students.

SCHOOL PROCEDURES

118) All students, members of staff and other adults have a responsibility to use the school's computer system in a professional, lawful and ethical manner. To ensure that all users are fully aware of their responsibilities when using technology, they are required to read and sign the appropriate Acceptable Use appendix. Where possible, this is done electronically.

119) In the event of an online safety incident involving illegal activity, the school will follow the principles outlined in the school's Child Protection Policy.

120) Online safety incidents that involve inappropriate, rather than illegal, activity will be dealt with through the school's Behaviour, Anti-Bullying and Child Protection Policies.

121) Anyone who has any concern about the welfare and safety of a student must report it

immediately to the DSL, in accordance with the school's Child Protection Policy and procedures.

122) The school reserves the right to withdraw access to the school's network by any user at any time and to report suspected illegal activity to the police.

123) Where staff identify technical deficiencies, or opportunities to improve the school’s filtering and monitoring systems they will report these via the IT Service Desk.

MONITORING AND EVALUATION

124) The school recognises that the digital landscape is a constantly changing environment with new apps, devices, websites and material emerging at a rapid pace. The school will:

a) regularly review filtering and monitoring data to identify, assess, and proactively respond to online risks; and
b) evaluate new technologies, completing appropriate risk assessments before their use is approved.

125) The Online Safety Lead will lead an annual review of the school’s filtering and monitoring provision using the Trust’s Online Safety Annual Audit Template, which aligns with the DfE’s Filtering and Monitoring Standards. Findings will be shared with the DSL, Principal/Headteacher and Regional IT Manager, and reported to the CET Safeguarding and IT Directorates.

126) The CET Safeguarding and IT Directorates will, through the scheme of Quality Assurance, provide assurance to the Safeguarding Committee that filtering and monitoring systems are effective across the Trust.

RECORD KEEPING

127) All records created under this policy, including online safety incidents and monitoring data, will be managed and retained in line with the school’s Data Protection Policy and Records Management and Retention procedures.

Appendix 1: Acceptable Use Policies

Staff Acceptable Use Policy

As a professional organisation with safeguarding responsibilities, the school requires all staff to take appropriate measures to protect data and information systems from unauthorised access, loss, abuse, or theft. All staff must use the school's technology and online services in a professional, lawful, and ethical manner. To ensure these expectations are understood, all staff are required to read and sign this Acceptable Use Policy.

This is not an exhaustive list. All members of staff are reminded that their use of ICT must be consistent with the school's ethos, policies, and applicable national and local guidance, as well as the law.

All references to "school" include the school and Creative Education Trust.

1) I understand that Information Systems and IT include networks, data and data storage, online and offline communication technologies, AI tools, and access devices. Examples include laptops, mobile phones, tablets, digital cameras, email and social media sites.

2) School-owned information systems must be used appropriately. I understand that the Computer Misuse Act 1990 makes the following criminal offences: to gain unauthorised access to computer material; to gain unauthorised access to computer material with intent to commit or facilitate commission of further offences or to modify computer material without authorisation.

3) I understand that any hardware and software provided by my workplace for staff use can only be used by members of staff and only for educational use. To prevent unauthorised access to systems or personal data, I will not leave any information system unattended without first logging out or locking my login as appropriate. I will protect the devices in my care from unapproved access or theft.

4) I will respect system security and I will not disclose any password or security information. I will use a 'strong' password; a strong password consists of 8 or more characters which contain at least one character from three of the following character sets: number, upper case letter, lower case letter, symbol, and is not used for any non-school services.

5) I will not attempt to install any purchased or downloaded software, including browser toolbars, or hardware without permission from IT Support.

6) I will ensure that any personal data of students, staff or parents/carers is kept in accordance with the Data Protection Act, the CET Data Protection, Online Safety and AI policies:
   a) This means that all personal data will be obtained and processed fairly and lawfully, only kept for specific purposes, held no longer than necessary and will be kept private and secure with appropriate security measures in place, whether used in the

workplace, hosted online or accessed remotely.

b) Any data which is being removed from the school site must be encrypted by a method approved by the school.
c) Any images or videos of students will only be used as stated in the online safety policy and will always take into account parental consent.
d) The school's data protection lead and Regional IT Manager must be informed in the event of any data being lost, stolen, or inadvertently disclosed. For example, a laptop is stolen or a mobile phone is lost with personal data stored on it.

7) I will not store professional documents which contain school-related sensitive or personal information, including images, files and videos, on any personal devices, such as laptops, digital cameras and mobile phones. Where possible I will use the school's Office 365 platform or VPN to upload and access any work documents and files in a password protected environment.

8) I will not store any personal information on the school computer system including any school laptop or similar device issued to members of staff that is unrelated to school activities, such as personal photographs, files or financial information.

9) I will respect copyright and intellectual property rights.

10) I have read and understood the CET Online Safety Policy, which covers the requirements for safe IT use, including using appropriate devices, delivery of on-line lessons, safe use of social media websites and the supervision of students within the classroom and other working spaces.

11) I have read and understood the CET Artificial Intelligence (AI) Policy, which sets out the requirements for the safe and responsible use of AI tools, including the use of approved AI tools, the protection of personal and sensitive data, the application of AI in teaching and learning and the duty to exercise professional judgement when using AI outputs.

12) I will follow CET guidance when setting up online lessons to ensure that appropriate safeguarding settings are in place, to prevent unauthorised use/access to online lessons.

13) I will immediately report any illegal, inappropriate or harmful material or incidents I become aware of to the DSL, as soon as possible.

14) I will not reply to, click on links, or open attachments in emails unless I am confident the message is genuine, expected, and safe. Recognising that emails from known contacts may still be malicious, I will verify unexpected messages and, if unsure, check with or report the email to IT Support immediately.

15) I will not attempt to bypass any filtering and/or security systems put in place by the school. If I suspect a computer or system has been damaged or affected by a virus or other malware, or if I have lost any school related documents or files, I will report it to IT Support immediately.

16) My electronic communications with current or past students, parents/carers and other professionals will take place within clear and explicit professional boundaries and will be

transparent and open to scrutiny at all times. All communication will take place via school approved communication channels such as a school provided email address or telephone number, and not via personal devices or communication channels, such as personal email, social networking or mobile phones.

17) I will ensure that my online reputation and use of IT and information systems are compatible with my professional role, whether using school or personal systems. This includes the use of email, text, social media, social networking, gaming and any other devices or websites.

18) I will take appropriate steps to protect myself online as outlined in the online safety policy and will ensure that my use of IT and the internet will not undermine my professional role, interfere with my work duties and will be in accordance with the school code of conduct and the law.

19) I will not create, transmit, display, publish or forward any material online that is likely to harass, cause offence, inconvenience or needless anxiety to any other person, or anything which could bring my professional role, or the school, into disrepute.

20) I will promote online safety with the students in my care and will help them to develop a responsible attitude to safety online, system use and to the content they access or create.

21) If I have any queries or questions regarding safe and professional practise online either in school or off site, then I will raise them with the school's Online Safety Lead.

22) I understand that my use of the school information systems, including any devices provided by the school, school internet and school email may be monitored and recorded to ensure the safety of children and staff and to ensure policy compliance. This monitoring will be proportionate and conducted in accordance with data protection and privacy legislation.

23) I understand that the school may exercise its right to monitor the use of information systems, including internet activity and emails, in order to monitor policy compliance. Where there is evidence or suspicion of unauthorised, inappropriate, or unacceptable use or behaviour, the school may apply its disciplinary procedures. Where criminal activity is suspected, the matter may be referred to the relevant law enforcement authorities.

I have read, understood and agree to comply with Creative Education Trust's Staff Acceptable Use Policy.

PRINT NAME: ………………………………………………………………………………………………..

SIGNED: …………………………………………………………………………………………………

JOB TITLE: ………………………………………………………………………………………..……..…

DATE: …………………………………………………………………………………………..……..

Visitor/Volunteer Acceptable Use Policy

As a professional organisation with responsibility for safeguarding it is important that all members of the school community are fully aware of their professional responsibilities and read and sign this Acceptable Use Policy.

This is not an exhaustive list; all members of the school community are reminded that ICT use should be consistent with the school ethos, school policies, national/local guidance and expectations, and the law.

All references to school include the school and Creative Education Trust.

1) I will ensure that any personal data of students, staff or parents/carers is kept in accordance with The Data Protection Act and the school's Data Protection Policy. Any data which is being removed from the school site, such as via email or on memory sticks, will be encrypted by a method approved by the school. Any images or videos of students will only be used as stated in the school's online safety policy and will always take into account parental consent.

2) I have read and understood the school online safety policy which covers the requirements for safe ICT and AI use, including using appropriate devices, safe use of social media websites and the supervision of students within the classroom and other working spaces.

3) I will follow the school's policy regarding confidentially, data protection and use of images and will abide with copyright and intellectual property rights, child protection legislation, privacy and data protection law and other relevant civil and criminal legislation.

4) I will respect system security and I will not disclose any password or security information that is given to me. To prevent unauthorised access to systems or personal data, I will not leave any information system unattended without first logging out or locking my login as appropriate.

5) My electronic communications with students, parents/carers and other professionals will only take place within clear and explicit professional boundaries and will be transparent and open to scrutiny at all times. All communication will take place via school approved communication channels such as via a school provided email address or telephone number and not via personal devices or communication channels such as via personal email, social networking or mobile phones.

6) My use of ICT and information systems will be compatible with my role within school. This includes the use of email, text, social media, social networking, gaming, web publications and any other devices or websites. I will take appropriate steps to protect myself online and my use of ICT will not interfere with my work duties and will always be in accordance with this Acceptable Use agreement and the law.

7) I will not create, transmit, display, publish or forward any material that is likely to harass, cause offence, inconvenience or needless anxiety to any other person, or anything which could bring my professional role, the school, into disrepute.

8) I will promote online safety with the children in my care and will help them to develop a responsible attitude to safety online, system use and to the content they access or create.

9) If I have any queries or questions regarding safe and professional practice online either in school or off site, I will raise them with the school's Online Safety Lead, DSL or the Principal/Headteacher.

10) I will report any incidents of concern regarding online safety to the school's Online Safety Lead or DSL as soon as possible.

11) I understand that if the school believes inappropriate use or unacceptable behaviour is taking place, the school may refuse me any further access. If the school suspects criminal offences have occurred, the matter will be brought to the attention of the relevant law enforcement organisation.

I have read, understood and agree to comply with Creative Education Trust's Visitor/Volunteer Acceptable Use Policy.

PRINT NAME: ……………………………………………………………………………………………………..

SIGNED: ………………………………………………………………………………………………………

JOB TITLE: …………………………………………………………………………………………..………

DATE: ……………………………………………………………………………………………………..…….

Student Acceptable Use Policy (KS3/4/5)

SAFE

- I will make sure that my internet use is safe and legal and I am aware that online actions have offline consequences.
- I know that my use of school computers, devices and internet access will be monitored to protect me and ensure I comply with the school's acceptable use policy.
- I will not use personal mobile data or create a 'hotspot' on any device to bypass the school's filtering and monitoring systems.
- I know that people online aren't always who they say they are and that I must always talk to an adult before meeting any online contacts.

PRIVATE

- I know I must always check my privacy settings are safe and private.
- I will think before I share personal information and/or seek advice from an adult.
- I will keep my password safe and private as my privacy, school work and safety must be protected.

RESPONSIBLE

- I will not access or change other people's files, accounts or information.
- I will only upload appropriate pictures or videos of others online and when I have permission.
- I will only use my personal device/mobile phone in school if I have permission from a teacher.
- I know I must respect the school's systems and equipment and if I cannot be responsible then I will lose the right to use them.
- I understand that any device that has been provided to me by the school is for my use only.
- I know that school computers and internet access has been provided to help me with my learning and that other use of technology may not be allowed. If I'm not sure if something is allowed then I will ask a member of staff.
- I will write emails and online messages carefully and politely; as I know they could be forwarded or seen by someone I did not intend.
- I will not install or attempt to install or store programmes of any type on any school device, nor will I try to alter computer settings.
- I know that use of the school's ICT system for personal financial gain, gambling, political purposes or advertising is not allowed.
- I understand that the school's internet filter is there to protect me, and I will not try to bypass it.
- I understand that any online meeting links that are shared with me, such as for on-line lessons are for my use only and I will not share these with anyone else.
- I understand that when I join an on-line meeting or lesson set up by the school that I must log in using my school account.
- I know that I must not record any lessons or meetings, using any means, such as using a phone or screen recording software.
- I know that when a recording of a lesson or meeting is made available by a member of staff that I must not download or upload it anywhere else.

- I know that if the school suspect that I am behaving inappropriately with technology, then enhanced monitoring and procedures may be used, such as checking and/or confiscating personal technologies such as mobile phones and other devices.
- I will only use AI tools that the school has approved for my schoolwork and will follow my teacher's instructions when using them. I will not use my own AI accounts for schoolwork.
- I know I must never use AI tools to upset or harm anyone, or to do anything inappropriate or against the law.

KIND

- I know that bullying in any form (on and off-line) is not tolerated and I know that technology should not be used for harassment.
- I will not upload or add any images, video, sounds or text that could upset, threaten the safety of or offend any member of the school community I will always think before I post as once I upload text, photos or videos they can become public and impossible to delete.
- I will not use technology to be unkind to people.

LEGAL

- I will respect other people's information and copyright by giving a reference and asking permission before using images or text from online sources.
- I understand that deliberately creating or sending false information intended to cause harm is a criminal offence. I will not knowingly share such harmful misinformation.
- I know it is a criminal offence to hack accounts or systems or to send threatening, offensive, or unsolicited sexual messages or images (known as cyberflashing).
- I understand that encouraging or assisting serious self-harm or suicide online is a criminal offence. I will not share or promote any content that instructs or encourages self-harm or suicide.
- I understand that it is a criminal offence, as well as a breach of school policy, to create, download, share or threaten to share inappropriate or harmful pictures, videos or other material online, including intimate images or sexually explicit deepfakes created without consent.

RELIABLE

- I will always check that any information I use online is reliable and accurate.
- I know that people I meet online may not be who they say they are. If someone online suggests meeting up then I will immediately talk to an adult and will always arrange to meet in a public place, with a trusted adult present.

REPORT

- If I am aware of anyone trying to misuse technology then I will report it to a member of staff.
- I will speak to an adult I trust if something happens to either myself or another student which makes me feel worried, scared or uncomfortable.
- I know that I can visit www.thinkuknow.co.uk, www.childnet.com and www.childline.org.uk to find out more about keeping safe online.

Student Acceptable Use Policy (KS2)

Safe

- I only send messages which are polite and friendly.
- I will only post pictures or videos on the internet if they are appropriate and if I have permission.
- I only talk with and open messages from people I know and I only click on links if I know they are safe.
- I know that people I meet online may not always be who they say they are. If someone online suggests meeting up, I will immediately talk to an adult.
- I know it is never okay to encourage someone to hurt themselves or others. If I see anything like that online, I will minimise it and tell a trusted adult straight away.

Trust

- I know that not everything or everyone online is honest or truthful and will check content on other sources like other websites, books or with a trusted adult.
- I understand that sharing lies or stories online to hurt someone is wrong. I will always check with a trusted adult if I'm unsure about something and will not share false information that could harm someone.
- I always credit the person or source that created any work, image or text I use.

Responsible

- I always ask permission from an adult before using the internet.
- I only use websites and search engines that my teacher has chosen.
- I use school computers for school work, unless I have permission otherwise.
- I ask my teacher before using my own personal devices/mobile phone.
- I keep my personal information safe and private online.
- I will keep my passwords safe and not share them with anyone.
- I will not access or change other people's files or information.
- I will only change settings on the computer if a teacher/technician has allowed me to.
- I will use my school account when joining on-line lessons.
- I will not share links to on-line lessons.

Understand

- I understand that the school's internet filter is there to protect me, and I will not try to bypass it.
- I know that my use of school devices and internet access will be monitored.
- I know that I can visit www.thinkuknow.co.uk, www.childnet.com and www.childline.org.uk to learn more about keeping safe online.

Tell

- If I am aware of anyone being unsafe with technology then I will report it to a teacher.
- I always talk to an adult if I'm not sure about something or if something happens online that makes me feel worried or frightened.
- If I see anything online that I shouldn't or that makes me feel worried or upset then I will minimise the page and tell an adult straight away.

Student Acceptable Use Policy (KS1)

- I only use the internet when an adult is with me.
- I only click on links and buttons online when I know what they do.
- I keep my personal information and passwords safe online.
- I only send messages online which are polite and friendly.
- I know the school can see what I am doing online.
- I always tell an adult/teacher if something online makes me feel unhappy or worried.
- I can visit www.thinkuknow.co.uk to learn more about keeping safe online.

Wi-Fi Acceptable Use Policy (Guest and Bring your own device access)

As a professional organisation with responsibility for safeguarding it is important all members of the school community are fully aware of the School boundaries and requirements when using the school Wi-Fi systems, and take all possible and necessary measures to protect data and information systems from infection, unauthorised access, damage, loss, abuse and theft.

This is not an exhaustive list; all members of the school community are reminded that ICT use should be consistent with the school ethos, school policies, national/local guidance and expectations, and the law.

All references to School include the school and Creative Education Trust.

1) The School provides Wi-Fi for the School community and allows temporary guest access for visitors and BYOD (Bring your own device) access for staff and sixth form students.

2) I am aware that the school will not be liable for any damages or claims of any kind arising from the use of the wireless service. The school takes no responsibility for the security, safety, theft, insurance and ownership of any device used within the school premises that is not the property of the school or is not part of a student 1 to 1 device scheme.

3) The use of ICT devices falls under the school's Acceptable Use Policy and Online Safety Policy which all students, staff and other adults must agree to, and comply with.

4) The school reserves the right to limit the bandwidth of the wireless service, as necessary, to ensure network reliability and fair sharing of network resources for all users.

5) School-owned information systems, including Wi-Fi, must be used lawfully and I understand that the Computer Misuse Act 1990 makes the following criminal offences: to gain unauthorised access to computer material; to gain unauthorised access to computer material with intent to commit or facilitate commission of further offences or to modify computer material without authorisation.

6) I will take all practical steps necessary to make sure that any equipment connected to the school's service is adequately secure, such as ensuring that connected equipment has up-to-date anti-virus software and system updates.

7) Use of the school's wireless service is done at my own risk. By using this service, I acknowledge that security errors and hacking are an inherent risk associated with any wireless network. For that reason, I expressly agree that I knowingly assume such risk and further agree to hold the school harmless from any claim or loss arising out of, or related to, any such instance of hacking or other unauthorised use or access into my

computer or device.

8) The school accepts no responsibility for any software downloaded and/or installed, e-mail opened, or sites accessed via the school's wireless service's connection to the internet. Any damage done to equipment for any reason including, but not limited to, viruses, identity theft, spyware, plug-ins or other internet-borne programs is my sole responsibility; and I indemnify and hold harmless the school from any such damage.

9) The school accepts no responsibility regarding the ability of equipment, owned by myself, to connect to the school's wireless service.

10) I will respect system security and I will not disclose any password or security information that is given to me. To prevent unauthorised access to systems or personal data, I will not leave any information system unattended without first logging out or locking my login as appropriate.

11) I will not attempt to bypass any of the school's security and filtering systems or download any unauthorised software or applications.

12) My use of the school Wi-Fi will be safe and responsible and will always be in accordance with this Acceptable Use appendix and the law including copyright and intellectual property rights. This includes the use of email, text, social media, social networking, web publications and any other devices or websites.

13) I will not upload, download, access or forward any material which is illegal or inappropriate or may cause harm, distress or offence to any other person, or anything which could bring the school into disrepute.

14) I will report any online safety concerns, filtering breaches or receipt of inappropriate materials to the school's Online Safety Lead, DSL or IT Support as soon as possible.

15) If I have any queries or questions regarding safe behaviour online then I will discuss them with school's Online Safety Lead, DSL, or the Principal/Headteacher.

16) I understand that my use of the school's Wi-Fi will be monitored and recorded to ensure policy compliance in accordance with privacy and data protection legislation. If the school suspects that unauthorised and/or inappropriate use or unacceptable or inappropriate behaviour may be taking place, then the school may terminate or restrict usage. If the school suspects that the system may be being used for criminal purposes, the matter will be brought to the attention of the relevant law enforcement organisation.