THISTLEY HOUGH ACADEMY
Creative Education Trust

Online Safety Policy

Review date: November 2023
Reviewed by: Ruth Ingerfield-Lapsley
Ratified by: Noel Kennedy
Review date: November 2024

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.

The school's Online Safety Lead is Ruth Ingerfield-Lapsley

The School's ICT Curriculum lead is Mohammed Imtiaz

The School's IT Support lead is Pete Gibson

Contents

Principles 4
Regulatory Framework 4
Publication and availability of this policy 5
Scope and responsibilities 5
Induction and training 7
Education and the curriculum 8
Managing the IT infrastructure 9
Filtering and monitoring 10
Data security 11
Classroom Use 12
Use of Video Conferencing Technology 12
Use of Personal Devices and Mobile Phones 13
Digital Images and Videos 14
Social Media 15
Staff Personal Use of Social Media 15
Pupils' Personal Use of Social Media 16
Official Use of Social Media 16
School Procedures 17
Monitoring and evaluation 18
Record Keeping 18
Appendix 1: Acceptable Use Policies 19

Principles

1) Creative Education Trust (CET) is committed to providing a safe and secure environment for pupils, staff and visitors and promoting a climate where pupils 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) Child Protection policy
    b) Anti-Bullying Policy
    c) Behaviour for Learning Policy
    d) Data Protection Policy
    e) Staff Code of Conduct
    f) Whistleblowing Policy
    g) Data Protection Policy

6) This policy takes account of the welfare requirements for children under 5 years of age included in the Statutory framework for the early years foundation stage[1].

7) The policy applies to all members of the school community, including staff and volunteers, pupils, 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 pupils or any member of the school community or where the culture or reputation of the school is put at risk.

Regulatory Framework

8) This policy has been prepared to meet the school's responsibilities under:
    a) Education (Independent School Standards) Regulations 2014
    b) Statutory framework for the Early Years Foundation Stage (DfE, Sept 2023)
    c) Education and Skills Act 2008
    d) Children Act 1989
    e) Childcare Act 2006
    f) Data Protection Act 2018 and General Data Protection Regulation (UK GDPR)

[1] Early years foundation stage (EYFS) statutory framework (Sept 2023).

g) Equality Act 2010

9) This policy also has regard to the relevant Departmental guidance and advice, such as Keeping Children Safe in Education (2023).

Publication and availability of this policy

10) This policy is published on the school website.

11) This policy is available in hard copy on request.

12) This policy can be made available in large print or other accessible format if required.

Definitions

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

14) 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).

15) All references to parent or parents mean the natural or adoptive parents of the pupil (irrespective of whether they are or have ever been married, with whom the pupil lives, or whether they have contact with the pupil) as well as any person who is not the natural or adoptive parent of the pupil, but who has care of, or parental responsibility for, the pupil (e.g. foster carer / legal guardian).

Scope and responsibilities

16) CET's online safety lead is Ash Mudaliar.

17) 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 pupils and parents/carers.

18) This policy applies to all access to the internet and use of technology, including personal devices, and where pupils, staff or other individuals have been provided with school-issued devices for use off-site, such as work laptops, tablets or mobile phones.

19) 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.

20) The school's designated safeguarding lead will take lead responsibility for online safety and understanding the filtering and monitoring systems and processes in place.

21) The school's online safety lead:
   a) will act as a named point of contact on all online safety issues and liaise with other members of staff or other agencies, as appropriate.
   b) will always be available during term time and school hours for staff in school to

discuss any online safety concerns.

c) will keep up-to-date with current research, legislation and trends regarding online safety and communicate this with the school community, as appropriate.
d) will ensure all members of staff receive relevant and appropriate online safety training.
e) will work with staff to coordinate participation in local and national events to promote positive online behaviour, such as Safer Internet Day.
f) will ensure that online safety is promoted to parents, carers and the wider community, through a variety of channels and approaches.
g) will maintain records of online safety concerns, as well as actions taken, as part of the school's safeguarding recording mechanisms.
h) will report online safety concerns, as appropriate, to the leadership team, Governing Body, and the trust's online safety Lead.
i) will ensure that staff, pupils and parents/carers are aware of this policy and related acceptable use policies.

22) 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.
i) will take personal responsibility for professional development in this area.

23) The school's IT support team:
a) will provide technical support and perspective to the online safety lead and leadership team, especially in the development and implementation of appropriate online safety policies and procedures.
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.
e) will take personal responsibility for professional development in this area.

24) Pupils (at a level that is 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.

25) Parents:
    a) will read this policy and Acceptable Use appendices and encourage their children to adhere to it.
    b) will 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) will 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) will endeavour to identify changes in their child's behaviour that could indicate that their child is at risk of harm online.
    e) will seek help and support from the school, or other appropriate agencies, if they or their child have online safety concerns.
    f) will use school systems, such as learning platforms and other network resources, safely and appropriately.
    g) will take responsibility for their own awareness in relation to the risks and opportunities posed by new and emerging technologies.

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

Induction and training

26) As part of their induction, all new staff will be provided with a copy of this policy. They will also be introduced to the online safety lead who will explain their role and provide them with basic 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.

27) Where safeguarding incidents involve youth produced sexual imagery, staff will follow the principles laid out in the Academy Child Protection policy, and Keeping Children Safe in Education (2023).

28) All staff members will be provided with online safety updates as part of their routine safeguarding and child protection training including on specific safeguarding issues such as sharing nudes and semi-nude images and or videos, cyberbullying, radicalisation and dealing with harmful online challenges and online hoaxes.

29) 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

30) Pupils are 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.

31) Pupils are 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

32) Pupils are taught to be critically aware of the materials / content they access online and be guided to validate the accuracy of information.

33) Pupils are taught about the risks associated with using the technology and how to protect themselves and their peers from potential risks.

34) Pupils are taught how to recognise suspicious, manipulative, dishonest, bullying or extremist behaviour.

35) Pupils are taught the definition of cyberbullying, its effects on the victim and how to treat each other's online identities with respect.

36) Pupils are taught how to report cyberbullying and/or incidents that make pupils feel uncomfortable or under threat and how the school will deal with those who behave badly.

37) Pupils are taught the consequences of negative online behaviour.

38) Pupils are taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet.

39) Pupils are 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. Pupils are reminded of the importance of the Acceptable Use appendices in this policy on a regular basis.

40) In lessons where internet use is pre-planned, pupils are guided to sites checked as suitable for their use and processes are in place for dealing with any unsuitable material that is found in internet searches.

41) Where pupils are allowed to freely search the internet, staff are vigilant in monitoring the content of the websites the pupils visit. In such circumstances, staff will be mindful of the needs of those pupils, including providing additional support to pupils with SEND who may require additional support to stay safe online.

42) It is accepted that from time to time, for good educational reasons, pupils 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 IT Support temporarily remove specific websites from the filtered list for the period of study. Any request to do so should be raised via the IT Service Desk, with clear reasons for the need.

Managing the IT infrastructure

43) 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
    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) regularly checking files held on the school's network and technology
    h) the appropriate use of user logins and passwords to access the school network and technology to ensure that users ae properly authenticated and authorised:
        i) specific user logins and passwords will be enforced for all but the youngest users (Early Years Foundation Stage children).
    i) all users must log off or lock their screens/devices if systems are unattended.

44) 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 where possible to reduce the risk of unauthorised access.
    b) completing cyber security training.

Password Policy

45) 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.

46) Members of staff must not record passwords or encryption keys on paper or in an unprotected file.

47) Members of staff must use different passwords for different accounts, to ensure that other systems are not put at risk if one is compromised and should be different for systems used inside and outside of school.

48) From Year 1, all pupils are provided with their own unique usernames and passwords to access school systems; pupils are responsible for keeping their password private.

49) We 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 IT Support immediately if they are aware of a breach of security with their password or account.

School Website

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

51) 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.

52) Staff or pupils' personal information will not be published on the school's website; the contact details on the website will be the school address, email and telephone number.

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

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

Email

55) Access to school email systems will always take place in accordance with data protection legislation and in line with other policies, including: 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 IT Support.
    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 will not be used for setting up personal social media accounts.

56) 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 so that they can remote wipe the device

57) 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) Pupils will use school-provided email accounts for educational purposes.

Filtering and monitoring

58) The school will ensure that appropriate filtering and monitoring is in place and take all reasonable precautions to ensure that users can only access appropriate material.

59) 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.

60) The school will have age-appropriate filtering and monitoring systems in place, to limit

children's exposure to online risks.

a) Illegal content eg. child sexual abuse images is filtered by the filtering provider by actively employing the Internet Watch Foundation CAIC list.
b) The filtering system blocks 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.
c) Content lists are regularly updated and Internet use is logged and regularly monitored.
d) The filtering system provides appropriate filtering levels for different ages and groups of users such as staff, primary school pupils and secondary school pupils.
e) The filtering and monitoring systems are configured to send automated safeguarding alerts and reports to the online safety lead to help identify pupils who are likely to be at risk based on their usage of IT in school.
f) The online safety lead, where that individual is not also the designated safeguarding lead, will immediately advise the latter of any concern that emerges.

61) Due to the global and connected nature of the Internet, it is not possible to guarantee that unsuitable or offensive material cannot be accessed via a school computer or device.

62) 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.

63) Use of technology in this way is a serious breach of discipline and may constitute a serious criminal offence. Pupils 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.

Data security

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

65) 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 computers/devices, ensuring that they lock the computer/device if leaving it unattended, and that they properly "log-off" at the end of any session in which they are using personal data
c) transfer data using encryption and secure password protected devices
d) Follow the new software/online service request process on the IT 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 pupils, staff, members of the school community, or any other sensitive information into an Al tool unless it has been approved for secure use by the Trust
f) comply with the Data Protection Policy

66) Staff use of personal external storage devices such as USB memory sticks and portable hard drives is prohibited.
a) 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 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.

67) 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 Use

68) 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.

69) 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.

70) Members of staff, where possible, will evaluate websites, tools and apps fully before use in the classroom or recommending for use at home.

71) The school will use age-appropriate search tools such as Google Safe Search.

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

73) Supervision of pupils will be appropriate to their age and ability:
    a) Early Years Foundation Stage and Key Stage 1
        i) Pupils' 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 pupils' age and ability.
    b) Key Stage 2
        i) Pupils will use age-appropriate search engines and online tools.
        ii) Children will be directed by the teacher to online materials and resources which support the learning outcomes planned for the pupil's age and ability.
    c) Key Stage 3, 4, 5
        i) Pupils will be appropriately supervised when using technology, according to their ability and understanding.

Use of Video Conferencing Technology

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

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

76) When delivering on-line lessons, the following must be adhered to.
    a) Normally, no 1:1 activity with pupils, 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 using Teams. Any 1:1 Teams calls must be recorded using the record function with the recording being retained by the teacher. Pupils' cameras remain disabled.
    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) Pupils must have video cameras switched off.
    e) Live classes should be kept to a reasonable length of time, or the streaming may prevent the family 'getting on' with their day.
    f) Language must be professional and appropriate, including any family members in the background.
    g) Staff must only use platforms provided by the school to communicate with pupils.
    h) Staff should record, the length, time, date and attendance of any sessions held.
    i) 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

77) Mobile phones brought into school are entirely at the staff member's, pupil'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.

Pupils:

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

79) Pupils 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 pupil 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).

Staff:

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

81) 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: Child Protection Policy, Data Protection Policy and the Acceptable Use appendices in this policy.

82) 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.

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

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

85) 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 pupils 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

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

87) The school does not include the full names of pupils in online photographic materials or in the credits of any published school-produced video materials / DVDs.

88) Pupils are advised to be very careful about placing any personal photos on any ‘social’ online network space. They are taught to understand the need to maintain privacy settings so as not to make public, personal information.

89) Pupils are taught that posting photos which in the reasonable opinion of the Principal / Headteacher could amount to a criminal offence, or which brings the school into disrepute, on any form of social media or websites such as YouTube etc is a serious breach of discipline and will be subject to disciplinary procedures.

90) Pupils are taught that they should not post images or videos of others without their permission. They are taught about the risks associated with providing information with images (including the name of the file), that reveals the identity of others and their location, such as house number, street name or school. Pupils are advised about the need to keep their data secure and what to do if they are subject to bullying or abuse.

91) Sharing nudes and semi-nude images (sexting/youth produced sexual imagery):
a) Pupils are taught about the risks of sharing nudes and semi-nude images and how to report any concerns to a member of staff.

92) Upskirting:
a) Upskirting typically involves taking a picture under a person's clothing without them knowing, with the intention of viewing parts of their body or clothing, not otherwise visible, to obtain sexual gratification, or cause the victim humiliation, distress or alarm.

b) Upskirting is strictly prohibited, whether or not you are in the care of the school at the time the image is recorded.
c) Upskirting is a criminal offence. Attempting to commit an act of upskirting may also be a criminal offence e.g. if actions are taken to do something that is more than merely preparatory to committing the offence such as attempting to take a photograph on a telephone or camera but failing to do so because of lack of storage space or battery.
d) The school will treat incidences of upskirting as a breach of discipline and also as a safeguarding matter under the school's child protection procedures (see the school's Child Protection Policy and procedures).
e) If you are concerned that you have been a victim of upskirting, speak to a member of staff for advice.

Social Media

93) 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.

94) The school will control pupil 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

95) 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.

96) 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.

97) 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.

98) 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.

99) 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.
   a) Information and content that staff members have access to as part of their employment, including photos and personal information about pupils and their family members or colleagues will not be shared or discussed on social media sites.

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

101) Members of staff must take all reasonable steps to ensure the proper separation of their professional and personal lives.

Communicating with pupils, parents and carers

102) All members of staff are advised not to communicate with or add as 'friends' any current or past pupils or current or past pupils' 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 pupils is required once they have left the school, members of staff will be expected to use official school-provided communication tools.

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

Pupils' Personal Use of Social Media

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

105) Any concerns regarding pupils' 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.

106) Pupils 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

107) 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.

108) 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.

109) 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.

110) 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

111) 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.

112) 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, pupils, 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 pupils.

School Procedures

113) All pupils, 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.

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

115) 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, as appropriate.

116) Anyone who has any concern about the welfare and safety of a pupil must report it immediately to the DSL in accordance with the school's Child Protection Policy and procedures.

117) 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.

118) 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

119) The school recognises that the internet is a constantly changing environment with new apps, devices, websites and material emerging at a rapid pace. The school will:
a) regularly review the methods used to identify, assess and minimise on-line risks
b) examine emerging technologies for educational benefit and undertake appropriate risk assessments before use in school is permitted

120) The school will review the filtering and monitoring provision and associated processes at least annually, or when there has been a significant implementation or change to the technology used at the school.

121) The Academy Council (AC), or Academy Improvement Board (AIB) in the absence of an AC, will appoint a safeguarding governor who will visit the school regularly and meet with the online safety lead. They will provide a report at each AC/AIB meeting using the CET safeguarding visit template to support CET in fulfilling its requirement to ensure that the school's arrangements for online safety are effective.

122) The CET Safeguarding Directorate will, through the scheme of Quality Assurance offer assurances to the Safeguarding Committee that filtering and monitoring systems are effective across the Trust.

Record Keeping

123) All records created in accordance with this policy are managed in accordance with the school's policies that apply to the retention and destruction of records.

124) The information created in connection with this policy may contain personal data. The school's use of this personal data will be in accordance with the Data Protection Policy.

Appendix 1: Acceptable Use Policies

Staff Acceptable Use Policy

As a professional organisation with responsibility for safeguarding it is important that staff take all possible and necessary measures to protect data and information systems from infection, unauthorised access, damage, loss, abuse and theft. All members of staff have a responsibility to use the school's computer system in a professional, lawful, and ethical manner. To ensure that members of staff are fully aware of their professional responsibilities when using technology, they are required to read and sign this Acceptable Use Policy.

This is not an exhaustive list; all members of staff 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 understand that Information Systems and IT include networks, data and data storage, online and offline communication technologies 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 only used on one system.

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 pupils, staff or parents/carers is kept in accordance with The Data Protection Act and the school's Data Protection Policy.
   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 pupils 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 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, VPN or Remote Desktop systems 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 school 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 pupils within the classroom and other working spaces.

11) I will 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.

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

13) I will not reply, click on links or open attachments in emails, unless I recognise the sender and know the content is safe. If you are unsure do not open the email and contact IT Support.

14) 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, then I will report this to IT Support as soon as possible.

15) My electronic communications with current or past pupils, 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.
a) 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.

16) 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.
a) 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/behaviour policy and the law.

17) 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.

18) I will promote online safety with the pupils 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.

19) 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.

20) 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 will take place in accordance with data protection, privacy and human rights legislation.

21) I understand that the school may exercise its right to monitor the use of information systems, including internet access and the interception of emails, in order to monitor policy compliance. Where it believes unauthorised and/or inappropriate use or unacceptable or inappropriate behaviour may be taking place, the school may invoke its disciplinary procedures. 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 Thistley Hough Academy Staff Acceptable Use Policy.

Print Name: …….. Job Title: ……..

Signed: ……..... 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 pupils, 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 or CDs, will be encrypted by a method approved by the school. Any images or videos of pupils 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 use, including using appropriate devices, safe use of social media websites and the supervision of pupils 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 pupils, 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.
    a) 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 appendix 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 Thistley Hough Academy Visitor/Volunteer Acceptable Use Policy.

Print Name: ……..

Signed: …….... Date: …….

Pupil 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 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 on-line 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.

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 know it can be a criminal offence to hack accounts or systems or send threatening and offensive messages.
- 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 it may be a criminal offence or breach of the school policy to download or share inappropriate pictures, videos or other material online.

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 pupil 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.

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 pupils.

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 pupil 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 pupils, 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.