E-safety Policy

The Academy's e-safety lead is David Thompson

The Academy's deputy e-safety leads are Claire Lewis & Daniel Shillito

The Academy's ICT Curriculum lead is Sandip Dosanjh

The Academy's ICT Support lead is Daniel Shillito

Contents

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) CET identifies that the issues classified within online safety are considerable, but can be broadly categorised into three 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

3) This policy should be read and implemented in conjunction with the child protection policy, anti-bullying policy, behaviour for learning and data protection policy.

4) 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].

5) The policy is applicable to all on- and off-site activities undertaken by pupils whilst they are the responsibility of the school.

Scope and responsibilities

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

7) CET's e-safety lead is Ash Mudaliar.

8) 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.

9) 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.

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

[1] Statutory framework for the early years foundation stage, Department for Education, March 2017

11) The school's e-safety lead:
    a) will act as a named point of contact on all e-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 e-safety concerns.
    c) will keep up-to-date with current research, legislation and trends regarding e-safety and communicate this with the school community, as appropriate.
    d) will ensure all members of staff receive regular, up-to-date and appropriate e-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 e-safety is promoted to parents, carers and the wider community, through a variety of channels and approaches.
    g) will maintain records of e-safety concerns, as well as actions taken, as part of the schools safeguarding recording mechanisms.
    h) will report e-safety concerns, as appropriate, to the leadership team, Governing Body and Trust.
    i) will ensure that staff, pupils and parents/carers are aware of this policy and related acceptable use policies.

12) It is the responsibility of all members of staff to:
    a) read and adhere to the e-safety policy and acceptable use policy (AUP).
    b) take responsibility for the security of school systems and the data they use, or have access to.
    c) model good practice when using technology and maintain a professional level of conduct in their personal use of technology, both on and off site.
    d) embed e-safety education in curriculum delivery, wherever possible.
    e) have an awareness of a range of e-safety issues and how they may be experienced by the children in their care.
    f) identify e-safety concerns and take appropriate action by following the school's safeguarding policies and procedures.
    g) know when and how to escalate e-safety issues, including signposting to appropriate support, internally and externally.
    h) take personal responsibility for professional development in this area.

13) It is the responsibility of staff managing the technical environment to:
    a) provide technical support and perspective to the e-safety lead and leadership team, especially in the development and implementation of appropriate e-safety policies and procedures.
    b) 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) ensure that the schools filtering policy is applied and updated on a regular basis; responsibility for its implementation is shared with the leadership team.
    d) report any filtering breaches to the e-safety lead and leadership team, as well as, the school's web filtering provider or other services, as appropriate.

14) It is the responsibility of pupils (at a level that is appropriate to their individual age, ability and vulnerabilities) to:
    a) engage in age-appropriate e-safety education opportunities.
    b) read and adhere to the AUP.
    c) respect the feelings and rights of others both on and offline.
    d) take responsibility for keeping themselves and others safe online.
    e) seek help from a trusted adult, if there is a concern online, and support others that may be experiencing e-safety issues.

15) It is the responsibility of parents and carers to:
    a) read the AUP and encourage their children to adhere to them.
    b) support the school in their e-safety approaches by discussing e-safety issues with their children and reinforce appropriate, safe online behaviours at home.
    c) role model safe and appropriate use of technology and social media.
    d) abide by the school's AUP and identify changes in behaviour that could indicate that their child is at risk of harm online.
    e) seek help and support from the school, or other appropriate agencies, if they or their child encounter risk or concerns online.
    f) use school systems, such as learning platforms, and other network resources, safely and appropriately.
    g) take responsibility for their own awareness in relation to the risks and opportunities posed by new and emerging technologies.

Induction and training

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

17) The Principal/Headteacher will determine the level of information that will be provided to temporary staff and volunteers.

18) All staff members will be provided with e-safety updates as part of their routine safeguarding and child protection training.

19) The school will provide e-safety advice, guidance and training for parents/carers through the following methods:
    a) Introduction of the AUP to new parents/carers, to ensure that principles of e-safe behaviour are made clear.
    b) Information leaflets; in school newsletters; on the school web site.
    c) Suggestions for safe Internet use at home.
    d) Provision of information about national support sites for parents/carers.

20) All members of the school community are 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 school's AUPs and highlighted through a variety of education and training approaches.

Education and the curriculum

21) Pupils are taught about safeguarding, including e-safety, through teaching and learning opportunities within the curriculum. The details are included in the school's curriculum documentation.

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

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

24) Pupils are helped to understand the need for the pupil AUP and encouraged to adopt safe and responsible use both within and outside school.

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

26) Where pupils are allowed to freely search the internet, staff must be vigilant in monitoring the content of the websites the pupils visit.

27) 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 ICT Support temporarily remove those sites from the filtered list for the period of study. Any request to do so should be raised via the IT Helpdesk, with clear reasons for the need.

Managing the ICT infrastructure

28) The school takes appropriate steps to ensure the security of its information systems, including:
    a) virus protection being updated regularly.
    b) encryption for personal data sent over the Internet, taken off site or access 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 checking files held on the school's network.
    f) the appropriate use of user logins and passwords to access the school network:
        i) specific user logins and passwords will be enforced for all but the youngest users (Early Years Foundation Stage children).
    g) all users must log off or lock their screens/devices if systems are unattended.

Password Policy

29) 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.

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

31) 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.

32) 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.

33) 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 ICT Support immediately if you aware of a breach of security with your password or account.
    e) Only disclose your account password to authorised ICT support staff when necessary, and never to anyone else. Ensure that all personal passwords that have been disclosed are changed once the requirement is finished.

School Website

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

35) 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.

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

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

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

Email

39) 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 AUPs.

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 you are unsure you must contact ICT 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.

40) The use of school email on personal smartphones/tablets is permitted provided the following conditions are met:
    a) The device is protected by a PIN/Passcode
    b) The device has remote wipe capability
    c) ICT Support are informed immediately if the device is lost or stolen so that they can remote wipe the device

41) 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.

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

Internet filtering and monitoring

43) 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.

44) 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.

45) 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 e-safety lead to help identify pupils who are likely to be at risk based on their usage of IT in school.

46) Due to the global and connected nature of the Internet, it is not possible to

guarantee that unsuitable material cannot be accessed via a school computer or device.

Data security

47) Personal data will be collected, stored and processed in accordance with the General Data Protection Regulation (GDPR).

48) 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) Have agreement from leadership staff and the data protection lead prior to signing up to any new online systems (including any free of charge services).
    e) Comply with the data protection policy.

49) 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

50) CET schools use 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

51) All school-owned devices will be used in accordance with the school’s AUPs and with appropriate safety and security measures in place.

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

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

54) 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.

55) 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 online 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 Personal Devices and Mobile Phones

56) Mobile phones brought into school are entirely at the staff member's, pupil's & parents/carers' 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.

57) The use of personal mobile phones or cameras by pupils or 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.

58) 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, data protection and AUPs.

59) 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.

60) Members of staff are not permitted to use their own personal phones for contacting pupils or parents and carers.

61) 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.

62) 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

63) The school will gain parental/carer permission for use of digital photographs or video involving their child as part of the school agreement form when their daughter / son joins the school.

64) 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.

65) 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.

66) 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 identify 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.

67) The school will ensure that all images and videos shared online are used in accordance with the associated polices, including (but not limited to): the data protection policy, behaviour policy and AUPs.

Social Media

68) The expectations regarding safe and responsible use of social media applies to all members of CET.

69) The term social media may include (but is not limited to): blogs; wikis; social networking sites; forums; bulletin boards; online gaming; apps; video/photo sharing sites; chatrooms and instant messenger.

70) 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

71) Safe and professional behaviour will be outlined for all members of staff (including volunteers) as part of the staff AUP.

72) 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.

73) 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.

74) 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.

75) 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.

76) 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.

Communicating with pupils and parents and carers

77) 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 designated safeguarding lead 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.

78) Any communication from pupils and parents/carers received on personal social media accounts will be reported to the schools designated safeguarding lead.

Pupils’ Personal Use of Social Media

79) 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.

80) 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 anti-bullying, behaviour and child protection. Concerns will also be raised with parents/carers as appropriate, particularly when concerning underage use of social media sites or tools.

81) 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

82) The official use of social media sites, by the school, only takes place with clear educational or community engagement objectives, with specific intended outcomes.
    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.

83) Official school social media channels have been set up as distinct and dedicated social media sites or accounts for educational or engagement purposes only.
    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.

84) Official social media use will be conducted in line with existing policies, including: anti-bullying, child protection and data protection.
    a) All communication on official social media platforms will be clear, transparent and open to scrutiny.

85) 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

86) 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.

87) If members of staff are participating in online 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 designated safeguarding lead and/or the Principal/Headteacher of any concerns, such as criticism, inappropriate content or contact from pupils.

School Procedures

88) 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 policy in appendix 1, where possible this is done electronically.

89) In the event of an e-safety incident involving illegal activity, the school will:
    a) Inform the e-safety lead for incidents involving pupils, and inform the Principal/Headteacher for incidents involving staff.
    b) Secure and preserve all evidence and hardware.
    c) Report the incident to the appropriate agencies, such as: IWF, the Police or CEOP.
    d) Take internal action through the school's behaviour, anti-bullying and child protection policies, as appropriate.

90) E-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.

91) A log of all reported e-safety incidents will be maintained by the school's e-safety lead. E-safety incidents (with personal information omitted) will also be reported to the trust's e-safety lead.

Monitoring and evaluation

92) 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 online risks.
    b) Examine emerging technologies for educational benefit and undertake appropriate risk assessments before use in school is permitted.

93) The AC/RIB will appoint a safeguarding governor who will visit the school regularly and meet with the e-safety lead. He/she will provide a report at each AC/RIB meeting using the CET safeguarding visit template to support the trust in fulfilling its requirement to ensure that the school's arrangements for e-safety are effective.

94) The trust's e-safety lead will maintain a central log of all school e-safety incidents (omitting personal information) to identify any gaps and trends, and use this data to update policies and procedures, and to implement improvements to filtering and security of IT systems across all CET schools to prevent reoccurrence where possible.

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 does not contain a dictionary word 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 ICT Support.

6) I will ensure that any personal data of pupils, staff or parents/carers is kept in accordance with the General Data Protection Regulation (GDPR) 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 e-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 e-safety policy which covers the requirements for safe IT use, including using appropriate devices, safe use of social media websites and the supervision of pupils within the classroom and other working spaces.

11) I will immediately report any illegal, inappropriate or harmful material or incidents I become aware of, to the e-safety lead as soon as possible.

12) I will not open any links or attachments in emails, unless the source is known and trusted. If you are unsure do not open the email and contact ICT Support.

13) 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 ICT Support as soon as possible.

14) 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.

15) 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 e-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.

16) 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.

17) I will promote e-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.

18) 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 e-safety lead.

19) 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.

20) 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 The Hart School 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 General Data Protection Regulation (GDPR) 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 e-safety policy and will always take into account parental consent.

2) I have read and understood the school e-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 the school AUP 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 e-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 practise online either in school or off site, I will raise them with the school's e-safety lead or the Principal/Headteacher.

10) I will report any incidents of concern regarding e-safety to the school's e-safety lead as soon as possible.

11) I understand that if the school believes inappropriate use or unacceptable behaviour is taking place, the school may invoke its disciplinary procedure. 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 The Hart School 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 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 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.

Pupil 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.

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 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 the settings on the computer if a teacher/technician has allowed me to.

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/computers 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.

Pupil 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 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 e-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 unauthorized 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 the school AUP 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 e-safety concerns, filtering breaches or receipt of inappropriate materials to the school's e-safety lead or ICT 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 e-safety lead 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.