All Saints' CE Primary School

E-Safety Policy

Approved: February 2019

Review date: February 2023

Author: R Sugden/ A Webb

To create a secure and safe environment which develops technology skills and provides pupils with awareness of potential E-Safety scenarios that may arise.

Policy statement

New technologies have become integral to the lives of children and young people in today's society, both outside and within school.

The internet and other digital and information technologies are powerful tools, which open up new opportunities for everyone. These technologies can stimulate discussion, improve literacy and communication skills, promote creativity and increase awareness of context to promote effective learning. Children and young people should have an entitlement to safe internet access at all times.

However, the use of these new technologies can put young people at risk both inside and outside of school. Some of these dangers may include:

- Access to illegal, harmful or inappropriate images or other content
- Unauthorised access to/loss of/sharing of personal information
- Inappropriate communication/contact with others, including strangers
- Cyber-bullying
- Access to unsuitable video/internet games
- Potential for excessive use which may impact upon the social and emotional development and learning of the young person
- Plagiarism and copyright infringement
- Illegal downloading of music or video files
- An inability to evaluate the quality, accuracy and relevance of information on the internet
- The sharing/distribution of personal images without an individual's consent or knowledge
- The risk of being subject to grooming by those with whom they make contact on the internet

As with all of these risks, it is impossible to eliminate these risks completely. It is therefore essential, through good educational provision, to build pupils' awareness to the risks which they may be exposed, so that they have the confidence and understanding to seek advice and to deal with any risks in an appropriate manner.

Named Persons

The following people are Named Persons at our school:

Designated Safeguarding Lead (DSL): Mr Joseph Cooper (Deputy Headteacher)
Deputy DSL: Miss Lisa King (SENDCO)
Named Safeguarding Governors (NSG): Mrs Judith Osborne (foundation governor) and Mrs Carol Stewart (associate governor)

Any safeguarding related issues will be shared with one of the people named above who will take the appropriate action depending on the issue.

Monitoring the impact of the policy

The school will monitor the impact of the policy using:

- Logs of reported E-Safety incidents
- Smoothwall monitoring of network activity
- Forensic monitoring of network including weekly reports sent to the Head teacher
- Discussions at children's groups i.e. school council
- Monitoring planning and evidence of work

Roles and responsibilities

Governors:

Governors are responsible for the approval of the E-Safety policy and for the reviewing the effectiveness of the policy.

Head Teacher:

The role of the Head and Leadership team includes:

- The Head Teacher is responsible for ensuring the safety (including E-Safety) of members of the school community, though the teaching and learning aspects of e-safety, including training, will be supported by the ICT coordinator.
- The Head teacher is responsible for ensuring that the ICT Coordinator, Named Persons and other staff receive suitable CPD to enable them to carry out their duties and to train other colleagues as appropriate.
- The Head teacher is aware of the procedures to be followed in the event of a serious E-Safety allegation being made against a member of staff.
- The Head teacher will deal with any incidents of misuse by staff

ICT Coordinator:

The role of the ICT Coordinator includes:

- The day to day responsibility for E-Safety issues and has a leading role in establishing and reviewing the school's E-Safety policy.
- Ensuring that all staff are aware of the procedures that need to be followed in the event of an E-Safety incident taking place.
- Receiving and reporting reports of E-Safety incidents and recording all incidents in the E-Safety log.
- Ensuring that all incidents are dealt with according to the school behaviour policy and that the Head, Class Teacher, Parents and other parties are informed where appropriate.

- Monitoring and reviewing the E-Safety teaching and learning taking place across the school.
- Being informed, when appropriate, of reports produced by forensic monitoring software of network activity.

Technician:
The school technician ensures:

- That the school's ICT infrastructures are secure and not open to misuse or malicious attack.
- That they keep up to date with E-Safety technical information and updates the ICT Coordinator as relevant.
- That monitoring software and antivirus software is implemented and updated.

Teaching and support staff
Teaching and support staff will:

- Keep an up to date awareness of E-safety matters and the current E-Safety policy through staff meetings and training sessions
- Read, understand and digitally accept the school Acceptable Use Policy annually (see appendix)
- Understand the process for reporting E-Safety incidents within the school including recording the incident in the E-Safety log
- Report any suspicious misuse or problem to the Head teacher / ICT Coordinator as appropriate for investigation
- Ensure that all digital communications with pupils should be professional and only carried out on official school systems.
- Ensure that E-Safety issues are embedded in all aspects of the curriculum
- Ensure that E-Safety lessons are incorporated into half termly computing topics and that the lessons are age appropriate/reflect the needs of the age group.
- Ensure that pupils understand and follow the school's Pupil Acceptable Use Policy. Training should be provided on these policies and this should be done on a regular cycle, including for new staff.
- Ensure that they are aware of the E-Safety issues related to the use of mobile phones, cameras and hand held devices and that they monitor their use and implement current school policies with regards to these devices.
- Ensure that confidential files are saved in an encrypted file and that the password for this file remains confidential.
- Ensure that at the end of the academic year photographs are deleted or where applicable stored in an agreed location for school use.

Named person(s) for child protection

The named persons responsible for child protection are trained in E-safety issues and are aware of the potential for serious child protection issues that may arise from:

- Sharing of personal data
- Access to illegal/inappropriate materials
- Inappropriate contact with adults/strangers
- Potential incidents of grooming
- Cyber-bullying

Pupils

Pupils are responsible for using the school ICT systems and equipment in accordance with the Pupil Acceptable Use Policy. They are briefed annually on the content of these policies which they are then asked to digitally accept.

Pupils are encouraged through E-Safety/PSHE lessons to share any E-Safety concerns with a trusted adult.

Parents/Carers

The school will take every opportunity to help parents/carers to understand E-Safety issues. We will raise awareness of the key issues in the following ways:

- Information about E-Safety and parental resources are available on the school website
- Information is also shared via letters and newsletters

Pupil Education

The education of pupils in E-Safety is a crucial part of the school's E-Safety provision. Children need the help and support of the school to recognise and avoid E-Safety risks and to build their awareness of how to keep themselves safe. E-Safety education will be provided in the following ways:

- Teachers plan for E-safety to be delivered as part of their computing sessions. The Computing National Curriculum, along with the computing long term planning, form the basis of all E-Safety teaching.
- Pupils are taught in all lessons to be aware of the content that they access online and learn how to validate the accuracy of the information they find.
- Rules for acceptable use are shared at the beginning of each academic year and with any new starters as they join school
- Pupils are taught how to search for information safely and safe search engines are used by Teaching Staff
- Pupils are taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet

- Copyright free images and audio sources are shared with the children and are included in the Bradford ICT Scheme of work
- Pupils are made aware of the process to follow if they see anything online which they find upsetting or which is unsuitable for children
- Pupils know that any events of Cyber-bullying are taken seriously by the school and they understand the importance of sharing their concerns with a trusted adult

Staff Education

It is essential that all staff receive regular E-Safety training and that they understand their responsibilities, as outlined in this policy. Training will be offered as follows:

- E-Safety staff training to be delivered annually by the ICT Coordinator or a member of the Bradford Council Curriculum Innovation Team.
- Training needs will be identified and used to plan staff training.
- Information and updates will be shared when necessary at staff meetings
- Planning and E-Safety work will be monitored regularly and will be used to direct training
- All staff will receive a briefing and a digital copy of the Acceptable use policy annually
- Staff will have access to the E-Safety policy and be notified of any amendments to the policy.
- New starters will be directed to the Acceptable Use Policy and E-Safety policy.

Governor Education

Governors are invited to take part in annual E-Safety training sessions with staff. These are delivered by the ICT Coordinator or by a member of the Bradford ICT team.

Internet provision

The school internet is provided by the Bradford Learning Network. All sites are filtered using the Smoothwall filtering system which generates reports on user activity. Forensic monitoring software is installed on our server and is used to monitor all computer use. Weekly reports are sent to the head teacher.

Managing ICT systems and access

Access to ICT systems is managed by the Technician. All children at the school receive logins and accounts for: school systems, email, Abacus Maths and Education City. These accounts are managed through administrator privileges which are only known to the Technician and ICT Coordinator. Accounts are created for new starters at the beginning of the academic year and then for new starters that join during the school year. Accounts of pupils who have left become inaccessible except for the Technician.

Adult accounts and passwords are also created in the same way. Adults are given accounts for school systems, email and other teaching resources such as Abacus Maths. Accounts of teachers who have left become inaccessible except for the Technician.

Passwords

All users (staff and pupils) have the responsibility for the security of their username and password and must not allow other users to access the systems using their log on details (as per Acceptable Use Policies). Any concerns about sharing passwords or log on details must be reported to the ICT Coordinator.

- Passwords for new users and replacement [passwords for existing users can be allocated by the Technician.
- Members of staff are made aware of the school's password rules through induction, the Acceptable Use Policy and the E-Safety policy.
- Pupils are made aware of the school's password rules through Computing/E-Safety lessons and through the Pupil Acceptable Use Policy.

All pupils have their own individual log in and password for accessing the school's ICT systems and school email accounts.

Personal Data Protection

Personal data will be recorded, processed, transferred and made available according to the General Data Protection Regulation (GDPR), 2018 which states that personal data must be:

- Fairly and lawfully processed
- Processed for limited purposes
- Adequate, relevant and not excessive
- Accurate
- Kept no longer than necessary
- Processed in accordance with the data subject's rights
- Secure
- Only transferred to others with adequate protection.

All staff must ensure the:

- Safe keeping of personal data at all times to minimise the risk of its loss or use.
- Use personal data only on secure password protected computers and other devices, ensuring that they are properly "logged off" at the end of any session in which they are using personal data.

- Ensure that only encrypted memory sticks issued by school are used to store sensitive and confidential data.
- Ensure that information is saved on secure drives which are password protected
- Ensure that any personal data held is only retained where there is a legitimate business need or legal requirement to do so – all other personal data should be securely deleted.

Use of digital and video images (photographic and video)

- Staff should inform and educate pupils about the risk associated with the taking, use, sharing, publication and distribution of images.
- Staff are allowed to take digital/video images to support educational aims. These images should only be taken on school equipment; personal equipment should not be used for these purposes. All classes now have a class camera for this purpose.
- Parental permission to use photographs on the school website and in the press must be given. Permission slips are stored in the children's files and records are given to each class teacher.
- Teaching staff are responsible for storing photographs and images safely and securely. All images should be transferred to a secure area for use and deleted from the camera at the earliest convenience.
- There are occasions when the school authorises photographs to be taken in school by people who do not work within the school (professional photographers for class photographs, PTA for fundraising activities etc.). In these cases, parents are informed and will have the right to remove their child(ren) from these activities.

Management of assets

All ICT assets are recorded on an inventory spreadsheet. Assets that are damaged or surplus to requirements have data removed by the Technician before being collected and destroyed by a reputable company. Certificates are received and filed where this has taken place.

Responding to incidents of misuse

It is hoped that all members of the school community will be responsible users of ICT. However, there may be incidents when infringements of the policy could take place, through careless or irresponsible or, very rarely, through deliberate misuse.

If apparent or actual misuse appears to involve illegal activity such as:

- Child sexual abuse images
- Adult material which breaches the Obscene Publications Act
- Criminally racist material
- Other criminal conduct, activity or materials

Then staff should immediately follow the guidance highlighted in 'Actions upon discovering inappropriate or illegal material'. It is important that the device is not shut down as evidence could be erased but that it is removed to secure site. All matters should be reported immediately to the Head/E-Safety Coordinator.

If misuse has taken place which is not illegal it is important that any incidents are dealt with in a proportionate manner, and that members of the school community are aware that incidents have been dealt with. It is intended that incidents of misuse will be dealt with through normal behaviour/disciplinary procedures.

Whilst it is impossible to record possible sanctions for every eventuality a list of types of misuse and sanctions are included in the appendix to this policy.

Cyber bullying

Cyber bullying is the use of electronic communication to bully a person, typically by sending messages of an intimidating or threatening nature. Examples of electronic communication are social networking web sites and apps, texting, use of other mobile or tablet apps, email or online software.

Pupils are taught about cyber bullying through E-Safety and PSHE lessons. Pupils are encouraged to share concerns of cyber bullying with a trusted adult. The adults in school will support the child by:

- Collecting evidence of the bullying taking place by recording the date, time and where possible screen captures
- Advising the child not to forward on messages to other people as this will continue the bullying
- Advising the child not to reply to the messages

Full details of how the school manages incidences of bullying can be found in our Anti-Bullying policy. The school may report serious cyber bullying incidents to the Police.

Social Media

All Saints' Primary School uses social media in the following ways:

- A Parent Communication system is managed by the school office. This is used as a reminder service for parents using email and text communications.

All members of staff must keep their personal and professional lives separate on social media. Personal opinions should never be attributed to the school. Staff should not add parents, carers or pupils as friends (including those that have since left) on personal social media pages/sites. Staff should not engage in online discussions relating to school or school matters. Further to this, staff should ensure that formal channels of communication are used when entering into school related discussions.

Personal Mobile devices

Staff

Staff must not use mobile phones in lessons. During teaching time, while on playground duty and during meetings, mobile phones will be switched off or put on 'silent' or 'discreet' mode. Staff are able to use personal devices in the staffroom and in school spaces out of teaching time, for example during lunchtime. Except in urgent or exceptional situations, mobile phone use is not permitted during teaching time, while on playground duty and during meetings. In exceptional circumstances, for health and safety reasons, staff are able to use mobile phones on school trips. In accordance with the Acceptable Use Policy staff should not use personal devices for photography in school. Only School cameras or devices are to be used. Mobile phones should have appropriate security, i.e. be Passcode or Touch ID protected.

Pupils

School does not allow children to bring mobile phones into class. If a child has a legitimate reason for having a mobile phone in school, they must bring in a completed mobile phone permission form signed by their parent/carer. Phones must be handed in to the school office or class teacher at the start of the day and are returned at the end of the school day.

School mobile devices

The school has, and may have in the future, a variety of mobile devices such as tablets and netbooks. All of the statements included in the Acceptable Use Policy apply to these devices. Pupils know that they must not take pictures of other people without their permission. They are not allowed to download or install apps on any device. These devices are subject to the same levels of internet filtering as all the school computers accessed by children.

We have detailed Acceptable Use Policies for staff and pupils. These are included in the appendices of this policy.

Development and Review of this policy

The implementation of this policy will be monitored by the ICT Coordinator.

Monitoring of the policy will take place annually, or more regularly in light of any significant new developments in the use of technologies, new threats to E-Safety of incidents that have taken place.

Should serious E-Safety incidents take place, the head teacher will be notified as soon as possible.

The school may exercise its right to monitor the use of the school's information systems and Internet access, to intercept e-mail and to delete inappropriate materials where it

believes unauthorised use of the school's information system may be taking place, or the system may be being used for criminal purposes or for storing unauthorised or unlawful text, imagery or sound. (Regulation of Investigatory Powers Act 2000).

Appendices

1) Staff Acceptable Use Policy
2) Pupil Acceptable Use Policy

The following policies include statements regarding E-Safety: PSHE, Child Protection, Behaviour and Bullying etc
These are available to be viewed within school if required.

Appendix One

Staff Acceptable Use Policy

(Formally Acceptable Use of School ICT & Communications System Policy)

Policy Statement

The Governing Body recognises the use of its ICT and communications facilities as an important resource for teaching, learning and personal development and as an essential aid to business efficiency. It actively encourages staff to take full advantage of the potential for ICT and communications systems to enhance development in all areas of the curriculum and school administration. It is also recognised by the Governing Body that along with these benefits there are also responsibilities, especially for ensuring that children are protected from contact with inappropriate material.

To complement the data protection duties of the school there are duties shared by all staff, governors and volunteers because, as a professional organisation with responsibility for children's safeguarding, it is essential that all 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 Information Communication Technology and the school systems, they are asked to read and sign this Acceptable Use Policy.
This agreement covers all digital and physical data systems, e.g. the internet, intranet, network resources, learning platform, software, communications tools (online and offline), equipment (access devices) and paper records, whether printed or handwritten and however stored.

School's ICT systems may only be used for work related use, or personal/study use when authorised by the Headteacher. The Governing Body expects use of this equipment for any purpose to be appropriate, courteous and consistent with the expectations of the Governing Body at all times.

This policy document is to be issued to all staff on its adoption by the Governing Body and when new staff are provided with mobile phones and passwords giving access to the ICT network.

Policy Coverage

This policy covers the use by staff of all school owned ICT and communications equipment, examples of which include:

- Laptop and personal computers
- ICT network facilities
- Personal digital organisers and handheld computers,

- Mobile phones and phone/computing hybrid devices
- USB keys and other physical and on-line storage devices,
- Image data capture and storage devices including cameras, camera phones and video equipment.

This list is not exhaustive.
The policy covers the use of all ICT and communications equipment provided for work purposes and equipment which is on loan to staff by the school for their personal or study use.

The Use of School ICT and Communications Facilities

Use of School ICT Equipment
Staff who use the school's ICT and communications systems:

- must use it responsibly
- must keep it safe
- must not share and must treat as confidential any passwords provided to allow access to ICT equipment and/or beyond firewall protection boundaries
- must report any known breach of password confidentiality to the Headteacher or nominated ICT Co-ordinator as soon as possible
- must report known breaches of this policy, including any inappropriate images or other material which may be discovered on the school's ICT systems
- must report to the Headteacher any vulnerabilities affecting child protection in the school's ICT and communications systems
- must not install software on the school's equipment, including freeware and shareware, unless authorised by the school's ICT Co-ordinator
- must comply with any ICT security procedures governing the use of systems in the school, including anti-virus measures
- must ensure that it is used in compliance with this policy
- must not copy files containing pupil data onto flash memory devices (if this is unavoidable for logistical reasons such data must be encrypted and password protected using a school issued memory devise with permission from the ICT team).

Any equipment provided to a member of staff is provided for their professional use. Any use of the equipment by family or friends is not permitted and any misuse of the equipment by unauthorised users will be the responsibility of the staff member.

Whilst it is not possible to cover all eventualities, the following information is published as guidance for staff on the expectations of the Governing Body. Any breaches of this policy or operation of the school's equipment outside statutory legal compliance may be grounds for disciplinary action being taken.

E-mail and Internet and Communications systems usage

The following uses of the school's ICT system are prohibited and may amount to gross misconduct and could result in dismissal:

1. to make, to gain access to, or for the publication and distribution of inappropriate sexual material, including text and/or images, or other material that would tend to deprave or corrupt those likely to read or see it
2. to make, to gain access to, and/or for the publication and distribution of material promoting homophobia or racial or religious hatred
3. for the purpose of bullying or harassment, or for or in connection with discrimination or denigration on the grounds of gender, race, religious, disability, age or sexual orientation
4. for the publication and/or distribution of libellous statements or material which defames or degrades others
5. for the publication of material that defames, denigrates or brings into disrepute the school and/or its staff and pupils
6. for the publication and distribution of personal data without authorisation, consent or justification
7. where the content of the email correspondence is unlawful or in pursuance of an unlawful activity, including unlawful discrimination
8. to participate in online gambling
9. where the use infringes copyright law
10. to gain unauthorised access to internal or external computer systems (commonly known as hacking)
11. to create or deliberately distribute ICT or communications systems "malware", including viruses, worms, etc.
12. to record or monitor telephone or email communications without the express approval of the Governing Body (or the Chair of Governors). In no case will such recording or monitoring be permitted unless it has been established for that such action is in full compliance with all relevant legislation and regulations (see Regulation of Investigatory Powers Act 2000, below).
13. to enable or assist others to breach the Governors expectations as set out in this policy.

Additionally, the following uses of school ICT facilities are not permitted and could lead to disciplinary action being taken:

1. for participation in "chain" email correspondence (including forwarding hoax virus warnings)
2. in pursuance of personal business or financial interests, or political activities (excluding the legitimate activities of recognised trade unions)
3. to access ICT facilities by using another person's password, or to post anonymous messages or forge email messages using another person's identity.

Note:
The above restrictions apply to the use of phones, emails, text messaging, internet chatrooms, blogs, and personal websites (including personal entries on MySpace, Facebook, Beebo, Twitter etc.).

Regulation of Investigatory Powers Act 2000

Ancillary to their provision ICT facilities the Governing Body asserts the employer's right to monitor and inspect the use by staff of any computer (including emails) or telephonic communications systems and will do so where there are grounds for suspecting that such facilities are being, or may have been, misused.

Appendix
Legal issues relevant to the use of ICT and communications equipment

Computer Misuse Act 1990
This was introduced as a means of prosecuting individuals who commit some form of computer crime. Hacking, eavesdropping, deliberate virus attacks are covered. Unauthorised access to a computer is the most likely offence within the Council. Only use machines/systems which you are authorised to use.

General Data Protection Act (GDPR) 2018 (Replacing Data Protection Act 1998)
Individuals have rights about personal data recorded on computer and in manual files. Don't put personal data in the subject line of emails; be careful about including it in the body of the text. An individual can request access to his personal data and this includes email. There are regulations about direct marketing via email.

Copyright, Design & Patents Act 1988
It is an offence to copy software without the author's permission. Downloading application software without permission or forwarding programs in attachments may put you in breach of this act. Some Internet sites will not let you copy material you find there Take care.

The Defamation Act 1996
Facts concerning individuals or organisations must be accurate and verifiable views or opinions must not portray their subjects in a way that could damage their reputation. This applies to internal as well as external email. Organisations in the UK have lost court cases where internal email systems were used to defame other organisations and heavy fines were imposed.

Protection from Harassment Act 1997
Accessing or distributing material which may cause offence to individuals or damage the Council's reputation may lead to a prosecution under these Acts. The fact that it is electronic does not prevent action.

Human Rights Act 1998
The present Government's commitment to incorporating the European Convention on Human Rights into domestic law has led to the introduction of the Human Rights Act 1998. Under this Act a UK citizen can assert their Convention rights through the national courts without having to take their cases to the European Court of Human Rights.

Obscene Publications Act 1959
All computer material is subject to the conditions of this Act, under which it is a criminal offence to publish an article whose effect, taken as a whole, would tend to deprave and corrupt those likely to read, see or hear it.

'Publish' has a wide meaning and is defined as including distributing, circulating, selling, giving, lending, offering for sale or for lease. It seems clear that material posted to a newsgroup or published on a World Wide Web page falls within the legal definition of publishing and is therefore covered by the Act. The publisher would appear to be the originator or poster of the item. The Council is the originator of the Bradford Internet & Intranet sites, or the Governing Body in the case of Voluntary Aided and Foundation schools.

Telecommunications Act 1984
The transmission of an obscene or indecent image from one computer to another via a 'public telecommunications system' is an offence under section 43 of this Act. For traditional mail, the same sort of offence is created under the Post Office Act 1953.

Protection of Children Act 1978;
Criminal Justice Act 1988
These Acts make it a criminal offence to distribute or possess scanned, digital or computer generated facsimile photographs of a child under 16 that are indecent.

Equality Act 2010
A new Equality Act came into force on 1 October 2010. The Equality Act brings together over 116 separate pieces of legislation into one single Act. Combined, they make up a new Act that provides a legal framework to protect the rights of individuals and advance equality of opportunity for all.

The Act simplifies, strengthens and harmonises the current legislation to provide Britain with a new discrimination law which protects individuals from unfair treatment and promotes a fair and more equal society.

Data Security Agreement

1. I understand that data held by the school may only be processed (acquired, processed, stored, deleted or transmitted) on the legal bases that the school has registered with the Information Commissioner's Office.
2. I will ensure that any personal data of pupils, staff or parents/carers is kept in accordance with the General Data Protection Regulation 2018. This means that all personal data will be 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. Any data which is being removed from the school site (such as via email or on memory sticks or CDs) will be encrypted. Any images or videos of pupils will always take into account parental consent. I will ensure that data no longer needed will be effectively deleted or shredded.
3. 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. Such misuse is also covered by the GDPR and any such misuse must be reported to the ICO, and to the data subjects (people) affected, within 72 hours.
4. 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 device as appropriate. I will not use personal equipment to access school data.
5. I will respect system security and I will not disclose any password or security information. I will use a 'strong' password. I will adopt school procedures for the safe storage of my passwords and for acquiring new ones.
6. I will not keep professional documents which contain school related sensitive or personal information (including images, files, videos etc.) on any personal devices (such as laptops, digital cameras, mobile phones). Where possible I will use the School [system] to upload any work documents and files in a password protected environment. I will protect the devices in my care from unapproved access or theft. I will not share any files or folders on the School [system] with any other user. I will be mindful that when working in a public space that others may be able to see my laptop, tablet or mobile phone screen and will use my discretion as to whether information should be hidden from site. I am aware that enabling Bluetooth connectivity on mobile devices can be a security threat and will switch this off when it is not needed for a specific connection.
7. I will not store any personal information on the school computer system that is unrelated to school activities, such as personal photographs, files or financial information.
8. I will respect copyright and intellectual property rights.

9. I have read and understood the school's and e-Safety Policy which covers the security of data and safe and appropriate access to data.
10. I will report all incidents of concern regarding children's online safety to the Designated Child Safeguarding Lead [DSL name and contact] and/or the e-Safety Coordinator [name and contact] and/or the lead for Prevent [name and contact] as soon as possible. I will report any accidental access, receipt of inappropriate materials, filtering breaches or unsuitable/extreme websites to the e-Safety Coordinator.
11. I will not attempt to bypass or alter any filtering and/or security systems put in place by the school.
12. My communications with pupils, parents/carers and other professionals will only take place via work approved communication channels e.g. via a school provided email address or telephone number. I will ensure that a BCC of any emails to parents/carers are sent to [school/office email address]. All written notes will be copied to [school/office contact]. Any pre-existing relationships which may compromise this will be discussed with the Senior Leadership team.
13. I will refrain from using any form of social media to discuss any aspect of school life except purely social events that involve colleagues. I will follow any guidance issued when contributing to the use of social media by the school as an official communication channel.
14. My use of ICT and information systems and my written communication will always be compatible with my professional role whether using school or personal systems. This includes the use of email, text, social media, social networking, gaming, web publications and any other devices or websites or postal addresses. My use of ICT and other forms of communication will not interfere with my work duties and will be in accordance with the school AUP and the Law.
15. I will not create, transmit, display, write, 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 or the school into disrepute.
16. I will promote e-Safety (including privacy) 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. Similarly, I will promote care for others in the pupils' writing and any other content that they create.
17. I understand that my use of the information systems, Internet and email may be monitored and recorded to ensure policy compliance.
18. 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 compliance with this Acceptable Use Policy and the School's E-Safety Policy. Where it believes unauthorised and/or inappropriate use of the service's information system or unacceptable or inappropriate behaviour may be taking place, the School will invoke its disciplinary procedure. If the School suspects that the system may be being used for criminal purposes or for storing unlawful text, imagery or sound, the matter will be brought to the attention of the relevant law enforcement organisation.

Staff Declaration

I confirm that I have read and understood the E-Safety Policy and the Staff Acceptable Use Policy.

Name ……

Signed ……

Date ……

Appendix Two

Our Pupil Acceptable Use Policy

The school provides computers with Internet access and a range of other equipment to help your learning. When using our ICT Network and associated equipment we have acceptable use rules. Following these rules will keep everyone safe and help us be responsible users.

- I will use only my own login and password, which I will keep secret;
- I will only access my own files.
- I will ask permission from a member of staff before using the Internet;
- I will use the computers only for school work and homework and other things that I have permission for;
- I will only access programs or internet sites which my teacher has told me to access;
- I will not bring CD-ROMs, DVDs, and Flash Memory Sticks into school unless I have permission and they are scanned before I use them.
- I will only email people I know, or my teacher has approved;
- The messages I send will be polite and sensible;
- I will not send or upload pictures or videos of myself or other children without my teacher's permission.
- I will not bring into school my own camera or other image capture devices (like phones) and take pictures.
- I will not give my full name, home address, phone number, or arrange to meet someone, unless my parent, carer or teacher has given permission;
- To help protect other pupils and myself, I will tell a teacher if I see anything I am unhappy with or I receive messages I do not like;
- I understand that I can use the internet for research but that I cannot copy and paste information or download video or music that is protected by copyright laws;
- I understand that the school may check my computer files and may monitor the Internet sites I visit.

I understand that breaking these rules can put all of us at risk, so anyone who does will not be able to use the school network.