Sherington Primary School
E-safety Policy

Our Vision Statement

Sherington Primary School is an inclusive community. We place the child at the centre of all that we do. We strive to maintain the highest standards in an environment that is creative, stimulating, inspiring and enabling.

Aspire

- Motivating and exciting all to become life-long learners

Believe

- Developing the skills and confidence to foster self-belief

Create

- Engaging all learners through creative practice and personal reflection

Achieve

- Experiencing success and embracing future challenges

Our Aims

To place the child at the centre of all that we do.
To foster positive, supportive relationships with families and the wider community.
To provide models of excellence drawing on the expertise of our highly skilled team.
To provide an enquiry based curriculum, that promotes the values of resilience, adaptability and perseverance.
To promote life-long learning through developing a whole school culture
of challenge and growth.
To prepare learners for a future in an increasingly interconnected global economy.

Policy Reviewed	April 2018
Agreed by Staff	June 2018
Ratified by Governors	June 2018
Date due for review:	June 2020

Sherington Primary School

E-safety Policy

Contents

Sherington Primary School
E-safety Policy

1 Policy Statement

1.1 Background

Sherington recognises that Information Technology (IT), and the Internet are excellent tools for learning, communication and collaboration. These are accessible within the school for enhancing the curriculum, to challenge pupils, and to support creativity and independence. Using IT to interact socially and share ideas can benefit everyone in the school community. However, it is important that the use of IT and the internet is understood and that it is the responsibility of pupils, staff and parents, to use it appropriately and practise good e-safety. It is important that all members of the school community are aware of the dangers of using the internet and how they should conduct themselves online.

1.2 Scope

E-safety does not just cover the internet and available resources, but all different types of devices and platforms (e.g. Smartphones devices, wearable technology and other electronic communication technologies). The school understands that some adults and young people will use these technologies to harm children. The school has a 'duty of care' towards any staff, pupils or members of the wider school community, to educate them on the risks and responsibilities of e-safety. It is important that there is a balance between controlling access to the internet and technology and allowing freedom to explore and use these tools to their full potential. This policy governs all individuals who use school systems. This could include staff, governors and pupils, however, sections of this policy may not be relevant to certain individuals due to their position, job role or subject to the age of the pupil.

2 Purpose

This policy aims to be an aid in regulating IT activity in school, and provide a good understanding of appropriate IT use that members of the school community can use as a reference for their conduct online outside of school hours. E-safety is a whole-community issue and responsibility.

Cyber-bullying by pupils will be treated as seriously as any other type of bullying and will be managed through the school's anti-bullying policy and procedures.

If there is a suggestion that a child is at risk of abuse or significant harm, the matter will be dealt with under the school's child protection procedures (see the school's safeguarding and child protection policy and procedures).

Sherington Primary School
E-safety Policy

3   Mandate

3.1   Roles and responsibility

The head, Designated Safeguarding Leads, Computing Lead and Governors will ensure that the e-safety policy is implemented and that compliance with the policy is monitored. The day-to-day management of e-safety in the school is the responsibility of the Computing Lead and SLT.

The Governing Body will undertake an annual review of the school's safeguarding procedures and their implementation, which will include consideration of how pupils may be taught about safeguarding, including online safety, through the school's curricular provision, ensuring relevance, breadth and progression.

The Pupil IT Acceptable Use Policy (Appendix A) is available to all parents/carers who are expected to read and adhere to it.

3.2   Communicating School policy including E-safety Week

A copy of the E-safety Policy is available on the school website for all to access, when and as they wish. E-safety is integrated into the curriculum in any circumstance where the internet or technology is being used, as well as being addressed in the computing curriculum. The annual E-safety Week is a vehicle to enhance the message of safe internet usage. On joining the school, new pupils and staff are required to agree to the Pupil/Staff IT Acceptable Use Policies (Appendix A and B). Existing staff may on occasion be required to re-sign this policy when significant changes are made.

4   Making use of IT and the Internet in School

Using IT and the internet in school brings many benefits to pupils, staff and parents. The Internet is used to raise educational standards, to promote pupil achievement, to support the professional work of staff and to enhance technology the school's management functions. Technology is advancing rapidly and is now a large part of everyday life, education and business. The school will endeavour to equip pupils with all the necessary IT skills for them to progress confidently between the key stages, into secondary school transition.

In common with other media such as magazines, books and video, some material available via the internet is unsuitable for pupils (some age specific). The school will take all reasonable precautions to ensure that users access only appropriate material. However, due to the international scale and linked nature of internet content, it is not possible to guarantee that unsuitable material will never appear on a school computer or device connected to the school network. The school cannot accept liability for all the material accessed, or all consequences of internet access unless found to be negligent. However, the school will act swiftly and follow policy and procedures outlined in our Child Protection Policy should any unsuitable material be uncovered.

Sherington Primary School

E-safety Policy

4.1   Learning to evaluate internet content

With so much information available online, it is important that pupils learn how to evaluate internet content for accuracy and intent. This is approached by the school as part of digital literacy across all subjects in the curriculum. Pupils will be taught:

- to be critically aware of materials they read, and shown how to validate information before accepting it as accurate, (e.g. 'fake news' and misleading websites);

- to acknowledge the source of information used and to respect copyright;

- about the risks associated with using the internet and how to protect themselves and their peers from potential risks;

- how to recognise suspicious, bullying or extremist behaviour;

- the definition of cyberbullying, its effects on the victim and how to treat each other's online identities with respect;

- the consequences of negative online behaviour; and

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

If staff or pupils discover unsuitable sites then the URL, time, date and content must be reported to the Computing Lead and SLT. Any material found by members of the school community that is believed to be unlawful will be reported to the appropriate agencies via the Senior Leadership Team. Regular checks will take place to ensure that filtering services and e-safety processes are in place, functional and effective.

The NSPCC provide comprehensive advice and support on online safety: https://www.nspcc.org.uk/preventing-abuse/keeping-children-safe/online-safety/

Please refer to the School Website's E-Safety page for more information and resources for parents/carers and pupils on how to stay safe online including the 'CEOP' button on to report concerns directly to the Child Exploitation and Online Protection Centre who are dedicated to protecting children from harm online and offline.

5   Managing information systems

The school is responsible for reviewing and managing the security of the IT services and networks that it operates and takes the protection of school data and personal protection of the school community seriously. This means protecting the school network (as far as is practicably possible) against viruses, hackers and other external security threats. The security of the school information systems and users will be reviewed regularly by the IT technician and other third parties engaged with the school. Anti-Virus and Malware protection software will be updated regularly. Some safeguards that the school takes to secure computer systems are:

- Making sure that unapproved software is not downloaded or installed to any school computers.
- Files held on the school network will be regularly backed up and checked for viruses.
- The use of user logins and passwords to access the school network will be enforced and unique.
- Portable media containing school data or programmes will not be taken off-site without specific permission from the Senior Leadership Team.

Sherington Primary School

E-safety Policy

5.1 Emails

The school uses email internally for staff, and externally for contacting parents, and conducting day to day school business and is an essential part of school communication. Access in school to external personal email accounts may be blocked. The school has the right to monitor emails, attachments and their contents but will only do so if there is suspicion of inappropriate use.

5.2 Published content and the school website and mobile App

The School website is viewed as a useful tool for communicating school ethos and practice to the wider community. It is also a valuable resource for prospective parents and pupils, current parents, pupils and staff for keeping up-to-date with school news and events, celebrating whole-school achievements, personal achievements and promoting the School.

The website and school App is in the public domain and can be viewed by anybody online. Any information published on the website or App will be carefully considered in terms of safety for the school community.

Staff, pupils and parents should take care to not publish anything on the internet that might bring the school into disrepute including on social media. Parents will be referred to the proper channels of communication should an issue arise.

5.3 Policy and guidance of safe use of children's photos

Photographs and pupils' work bring the school to life, showcase pupils' talents, and add interest to publications both online and in print that represent the school. However, the school acknowledges the importance of having safety precautions in place to prevent the misuse of such material.

When parents/carers complete admissions paperwork, they consent to children's images to be used for school purposes. This may include images in:

- School publications
- On the school website or App
- Videos made by the school or in class for school projects

Parents who wish for their children to not to appear on the school website, social media or publications, who have previously agreed to do so, can opt out by putting a request in writing to the school office.

Images of certain children will not be used for external media where there are safeguarding concerns including looked-after children.

5.4   Photography and filming of children

Children will only be photographed while in school or doing school activities like educational visits. Photographs and videos at school will be taken by staff only.

The school follows general rules on the use of photographs and videos of children.

- Electronic and paper images will be stored appropriately.

- Staff will only use equipment provided or authorised by the school, (not their own device).

- Images will be carefully chosen to ensure that they do not pose a risk of misuse. This includes ensuring that pupils are appropriately dressed.

- For public documents, including in newspapers, full names will not be published alongside images of the child without the consent of the parents.

- Groups may be referred to collectively by year group/class name.

- It is the school's policy that parents do not film or photograph assemblies, concerts, performances or any other events – these, when appropriate, will be recorded by the school and posted on school communication platforms. This protects children who are not able to be filmed for safeguarding reasons, those whose parents/carers have not given consent and allows all children to participate in performances.

- Pupils are encouraged to tell a member of staff if they are concerned or uncomfortable with any photographs that are taken of them or they are being asked to participate in.

- Any photographers that are commissioned by the school will be fully briefed on appropriateness in terms of content and behaviour, will wear identification always, and will not have unsupervised access to the pupils.

5.5   Complaints of misuse of photographs or video

Parents should follow standard school complaints procedure if they have a concern or complaint regarding the misuse of school photographs. Please refer to the Complaints Policy (available on the website or school office) for more information on the steps to take when raising a concern or making a complaint. Any issues or sanctions will be dealt with in line with this policy.

6   Social networking, social media and personal publishing

Personal publishing tools include blogs, wikis, social networking sites, chat rooms and instant messaging programmes. These online forums are the more obvious sources of inappropriate and harmful behaviour and where pupils are most vulnerable to being contacted by a dangerous person. It is important that the school educates pupils so that they can make their own informed decisions and take responsibility for their conduct online. The school will normally block/filter access to social networking sites via the school network. The school encourages parents with children to follow the guidance of social media sites such as Facebook and not give their child access (children under the ages of 13 should not hold an account). Access to any such sites found by the school during their duty will be reported to parents and the website in question will be informed

of the account and a request made for its removal.

Social media sites have many benefits, however staff, parents and pupils should be aware of how they present themselves online. Pupils are taught through the computing curriculum about the risks and responsibility of uploading personal information and the difficulty of taking it down completely once it is out in such a public place. The school adheres to the following rules to ensure technology is used appropriately and online safety is promoted:

- Pupils are educated on the dangers of social networking sites and how to use them in safe and productive ways. Pupils are advised never to give out personal details of any kind which may identify them or their location.

- Any sites that are to be used in class will be risk-assessed by the teacher in charge prior to the lesson to ensure that the site is age-appropriate and safe for use.

- Pupils, parents and staff are encouraged not to publish specific and detailed private thoughts, especially those that might be considered hurtful, harmful or defamatory. The school expects all staff and pupils to remember that they are always representing the school and must act appropriately.

- Safe and professional behaviour of staff online will be discussed at staff induction and guidance is provided through the staff IT Acceptable Use Policy.

- Pupils, parents and staff are not permitted to use of personal social media platforms such as YouTube (personal accounts), Facebook, SnapChat or Instagram in school.

7 Mobile phones and personal mobile electronic devices (smartphones), including wearable technology

Mobile phones and other personal devices are now an important part of everyone's life and have considerable value, particularly in relation to individual safety. Whilst these devices are commonplace today, their use and the responsibility for using them should not be taken lightly. Some issues surrounding the possession of these devices are that:

- they can make pupils and staff more vulnerable to cyberbullying;
- they can be used to access inappropriate internet material;
- they can be a distraction in the classroom;
- they are valuable items that could be stolen, damaged, or lost; and
- they can have integrated cameras, which can lead to child protection, bullying and data protection issues.

The school's expectation is that with mobile devices certain measures are taken to ensure that staff and pupils adhere to this expectation. Staff must follow the IT Acceptable Use Policy for further guidance on this matter. Pupils cannot use mobile phones or have access to them at school. The school cannot accept any liability for any loss or damage to phones or devices.

8 Cyberbullying

Cyberbullying, as with any other form of bullying, is taken very seriously by Sherington. Information about specific strategies to prevent and tackle bullying are set out in the Anti-Bullying Policy. The anonymity that can come with using the internet can sometimes make people feel safe to say and do hurtful things that they otherwise would not do in person. It is made very clear to all members of the school community what is expected of them in terms of respecting their peers, members of the public and staff, and any intentional breach of this will result in disciplinary action. Our PSHE curriculum and school values reinforce positive behaviour to prevent and tackle bullying.

Any incidents of cyberbullying will be dealt with in accordance with the Anti-Bullying Policy and, where appropriate, the school's safeguarding and child protection policies and procedures. This includes incidents that the school becomes aware of that take place on school related activities, outside of school hours or off school premises.

9 Managing emerging technologies

Technology is progressing rapidly and innovative technologies are emerging all the time. The school will risk-assess any new technologies before they are allowed in school, and will consider any educational and teaching benefits that they might have. The school keeps up-to-date with modern technologies and is prepared to quickly develop appropriate strategies for dealing with new technological developments.

10 Protecting personal data

The school believes that protecting the privacy of staff, pupils, and parents and regulating their safety through data management, control and evaluation is vital to the whole school and individual progress. The school collects personal data from pupils, parents, and staff and processes it to:

- conduct day to day business processes (e.g. finance, human resources etc.);
- support teaching and learning;
- monitor and report on pupil and teacher progress;
- strengthen pastoral provision.

The School takes responsibility for ensuring that any personal data that is collected and processed is used correctly and only as is necessary. We will keep parents fully informed of how personal data is collected, what is collected, and how it is used. Results, attendance and registration records, special educational needs data, and any relevant medical information are examples of the type of personal data that the school processes.

In line with the Data Protection Act 1998, and following principles of good practice when processing data, the school will:

- ensure that data is fairly and lawfully processed;
- process data only for limited purposes;
- ensure that all data processed is adequate, relevant and not excessive;
- ensure that data processed is accurate;
- not keep data longer than is necessary or legally required;
- process the data in accordance with the data subject's rights;
- ensure that data is secure;
- ensure that data is not transferred to other countries without adequate protection.

The Data Protection Act will be superseded by the General Data Protection Regulation (GDPR) from 25th May 2018 and personal data will be managed in accordance to it.

Sherington Primary School

E-safety Policy

11 Asset disposal

Details of all school-owned hardware will be recorded in a hardware inventory. All redundant equipment will be disposed of through an authorised agency. This will include a written receipt for the item including an acceptance of responsibility for the destruction of any personal data. All redundant equipment that may have held personal data will have the storage media wiped. Alternatively, if the storage media has failed, it will be physically destroyed.

Sherington Primary School
E-safety Policy

Appendix A – Pupil IT Acceptable Use Policy

Sherington Pupil IT Acceptable Use Policy Agreement

Sherington recognises that Information Technology (IT) and the Internet are excellent tools for learning, communication and collaboration. These are accessible within the school for enhancing the curriculum, to challenge pupils, and to support creativity and independence. Using IT to interact socially and share ideas can benefit everyone in the school community. However, it is important that the use of IT and the internet is understood and that it is the responsibility of pupils, staff and parents, to use it appropriately and practise good e-safety. Young people should have an entitlement to be safe whilst using the internet and IT at all times.

This Acceptable Use Policy is intended to ensure:

- that young people will be responsible users and stay safe while using the internet and other digital technologies for educational, personal and recreational use;

- that school systems and users are protected from accidental or deliberate misuse that could put the security of the systems and users at risk.

The school will try to ensure that students will have good access to digital technologies to enhance their learning and will, in return, expect the students to agree to be responsible users.

Acceptable Use Policy Agreement

I understand that I must use school IT systems in a responsible way, to ensure that there is no risk to my safety or to the safety and security of the IT systems and other users.

For my own personal safety:

- I understand that the school will monitor my use of the systems, devices and digital communications.

- I will be aware of people not being who they actually say they are when I am communicating on-line.

- I will not disclose or share personal information about myself or others when on-line (this could include names, addresses, email addresses, telephone numbers, age, gender, educational details, financial details etc.)

- I will immediately report any unpleasant or inappropriate material or messages or anything that makes me feel uncomfortable when I see it on-line to a member of staff.

I understand that everyone has equal rights to use technology as a resource and:

- I understand that the school systems and devices are primarily intended for educational use and that I will not use them for personal or recreational use unless I have permission.

- I will not try (unless I have permission) to make large downloads or uploads that might take up internet capacity and prevent other users from being able to carry out their work.

- I will not use the school systems or devices for on-line gaming, on-line gambling, internet shopping, file sharing, or video broadcasting (e.g. YouTube), unless I have permission from a member of staff to do so.

Sherington Primary School

E-safety Policy

I will act as I expect others to act toward me:

- I will respect others' work and property and will not access, copy, remove or otherwise alter any other user's files, without the owner's knowledge and permission.
- I will be polite and responsible when I communicate with others, I will not use strong, aggressive or inappropriate language and I appreciate that others may have different opinions.

- I will not take or distribute images of anyone without their permission.

I recognise that the school has a responsibility to maintain the security and integrity of the technology it offers me and to ensure the smooth running of the school:

- I will not use my own personal devices (mobile phones/USB devices etc.) in school unless I have been given specific permission to do so from a member of staff. I understand that, if I am given permission to use my own devices in school, I will follow the rules set out in this agreement, in the same way as if I was using school equipment.

- I understand the risks and will not try to upload, download or access any materials which are illegal or inappropriate or may cause harm or distress to others, nor will I try to use any programmes or software that might allow me to bypass the filtering/security systems in place to prevent access to such materials.

- I will immediately report any damage or faults involving equipment or software, however this may have happened.

- I will not open any hyperlinks in emails or any attachments to emails, unless I know and trust the person/organisation who sent the email, or if I have any concerns about the validity of the email (due to the risk of the attachment containing viruses or other harmful programs).

- 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.

- In general the use of social media sites will not be permitted in school.

When using the internet for research or recreation, I recognise that:

- I should ensure that I have permission to use the original work of others in my own work.

- Where work is protected by copyright, I will not try to download copies (including music and videos).

- When I am using the internet to find information, I should take care to check that the information that I access is appropriate, and I understand that not all information on the internet is truthful and may be a deliberate attempt to mislead me.

I understand that I am responsible for my actions, both in and out of school:

- I understand that the school also has the right to take action against me if I am involved in incidents of inappropriate behaviour, that are covered in this agreement, when I am out of school and where they involve my membership of the school community (examples would be cyber-bullying, use of images or personal information).

- I understand that if I fail to comply with this Acceptable Use Policy Agreement, I will be subject to sanctions in line with the school behaviour policy which may result in loss of access to the school network/internet. Parents/carers will be contacted in the event of illegal activities alongside the involvement of the police if necessary.

Sherington Primary School

E-safety Policy

Parental Agreement

At Sherington, we value the use of IT and the internet as a learning tool and an integral aspect of a constantly evolving world we all live in. We believe that children have the right to use technology and the internet safely and in an appropriate way. We believe that both parents/carers and the school share a responsibility for our children's use of IT and the internet by teaching them how to use it safely, appropriately and respectfully. By signing below, you agree to allow your child to use the IT facilities and internet in school as is laid out in this agreement.

Name of Parent/Carer

Signed

Date

When children are older and have a greater understanding of the acceptable use of IT, they will sign the Acceptable Use Agreement Form. It will be signed in year 3, at the beginning of KS2, after a computing lesson on the acceptable use of IT and E-safety.

Pupil Acceptable Use Agreement Form

This form relates to the student Acceptable Use Agreement; to which it is attached.

I understand the above and agree to follow these guidelines when:

- I use the school systems and devices (both in and out of school).

- I use my own devices in the school (when allowed) e.g. mobile phones, USB devices, cameras etc.

- I use my own equipment out of the school in a way that is related to me being a member of this school community.

Name of Student

Signed

Date

Sherington Primary School
E-safety Policy

Appendix B – Staff IT Acceptable Use Policy

Sherington Staff (and Volunteer) IT Acceptable Use Policy Agreement

Rationale

Information technology (IT) and the internet is an essential element of modern education and social interaction. The purpose of ICT use in school is to promote child achievement, to support the professional work of staff and to enhance the school's management, information and business administration system. They also bring opportunities for staff to be more creative and productive in their work. All users should have an entitlement to safe internet access at all times.

This Acceptable Use Policy is intended to ensure:

- that staff and volunteers will be responsible users and stay safe while using the internet and other communications technologies for educational, personal and recreational use;

- that school systems and users are protected from accidental or deliberate misuse that could put the security of the systems and users at risk;

- that staff are protected from potential risk in their use of IT in their everyday work.

Acceptable Use Policy Agreement

I understand that I must use school IT systems in a responsible way, to ensure that there is no risk to my safety or to the safety and security of the IT systems and other users. I recognise the value of the use of IT for enhancing learning and will ensure that students receive opportunities to gain from the use of IT. I will, where possible, educate the young people in my care in the safe use of IT and embed online safety in my work with young people.

For my professional and personal safety:

- I understand that the school will monitor my use of the IT systems, email and other digital communications.

- I understand that the rules set out in this agreement also apply to use of school IT systems (e.g. laptops, email, website etc.) out of school, and to the transfer of personal data (digital or paper based) out of school.

- I understand that the school IT systems are primarily intended for educational use and that I will only use the systems for personal or recreational use within the policies and rules set down by the school.

- I will not disclose my username or password to anyone else, nor will I try to use any other person's username and password. I understand that I should not write down or store a password where it is possible that someone may steal it.

- I will immediately report any illegal, inappropriate or harmful material or incident, I become aware of, to the appropriate person.

I will be professional in my communications and actions when using school ICT systems:

- I will not access, copy, remove or otherwise alter any other user's files, without their express permission.

Sherington Primary School

E-safety Policy

- I will communicate with others in a professional manner, I will not use aggressive or inappropriate language and I appreciate that others may have different opinions.

- I will ensure that when I take and/or publish images of others I will do so with their permission and in accordance with the school's policy on the use of digital/video images. I will not use my personal equipment to record these images, unless I have permission to do so. Where these images are published (e.g. on the school website) it will not be possible to identify by name, or other personal information, those who are featured.

- I will only use social networking sites in school in accordance with the school's policies.

- I will only communicate with students and parents/carers using official school systems. Any such communication will be professional in tone and manner. I will not use my personal email addresses, mobile phones or social media accounts for such communications.

- Sherington is a creative school which encourages the use of new and existing technology. If I wish to use social media in my teaching I will email the Computing Lead with details so it can be discussed and logged.

- I will not engage in any on-line activity that may compromise my professional responsibilities (for example, use the privacy settings on Facebook to ensure staff have control over who views their profile).

The school and the local authority have the responsibility to provide safe and secure access to technologies and ensure the smooth running of the school:

- When I use my mobile devices (PDAs/ laptops/mobile phones/USB devices etc.) in school, I will follow the rules set out in this agreement, in the same way as if I was using school equipment. I will also follow any additional rules set by the school about such use. I will ensure that any such devices are protected by up to date anti-virus software and are free from viruses.

- I will not use personal email addresses on the school IT systems.

- I will not open any hyperlinks in emails or any attachments to emails, unless the source is known and trusted, or if I have any concerns about the validity of the email (due to the risk of the attachment containing viruses or other harmful programs).

- I will ensure that my data is regularly backed up, in accordance with relevant school policies.

- I will not try to upload, download or access any materials which are illegal (child sexual abuse images, criminally racist material, adult pornography covered by the Obscene Publications Act) or inappropriate or may cause harm or distress to others. I will not try to use any programs or software that might allow me to bypass the filtering/security systems in place to prevent access to such materials.

- I will not try (unless I have permission) to make large downloads or uploads that might take up internet capacity and prevent other users from being able to carry out their work.

- I will not install or attempt to install programs of any type on a machine, or store programs on a computer, nor will I try to alter computer settings, unless this is allowed in school policies.

- I will not disable or cause any damage to school equipment, or the equipment belonging to others.

- Where digital personal data is transferred outside the secure local network, it must be encrypted. Paper based Protected and Restricted data must be held in lockable storage.

- I understand that data protection policy requires that any staff or student data to which I have access,

will be kept private and confidential, except when it is deemed necessary that I am required by law or by school policy to disclose such information to an appropriate authority.

- I will immediately report any damage or faults involving equipment or software, however this may have happened.

When using the internet in my professional capacity or for school sanctioned personal use:

- I will ensure that I have permission to use the original work of others in my own work.

- Where work is protected by copyright, I will not download or distribute copies (including music and videos).

I understand that I am responsible for my actions in and out of the school:

- I understand that this Acceptable Use Policy applies not only to my work and use of school IT equipment in school, but also applies to my use of school IT systems and equipment off the premises and my use of personal equipment on the premises or in situations related to my employment by the school.

- I understand that if I fail to comply with this Acceptable Use Policy Agreement, I could be subject to disciplinary action. This could include a warning, a suspension, referral to Governors or the Local Authority and in the event of illegal activities, the involvement of the police.

I have read and understand the above and agree to use the school IT systems (both in and out of school) and my own devices (in school and when carrying out communications related to the school) within these guidelines.

Staff/Volunteer Name

Signed

Date

Sherington Primary School

E-safety Policy

Sherington Primary School

E-safety Policy

Sherington Primary School

E-safety Policy