Bevington Primary School

Online Safety Policy

September 2019

1. Introduction and Overview

This Online Safety Policy sets out the roles, responsibilities and procedures for the acceptable, safe and responsible use of all digital and communication technologies, including the use of school based devices, the internet, email, instant messaging and other social networking, mobile phones, online games/gaming, to safeguard all pupils, staff and the community of Bevington. The policy details how the school will provide support and guidance to parents and the wider community for the safe and responsible use of these technologies. It also explains procedures for any unacceptable or misuse of these technologies by staff or pupils.

The Online Safety Policy works in conjunction with our school Child Protection and Safeguarding policy.

Why have an Online Safety Policy?

The use of the internet as a tool to develop teaching, learning, administration and to prepare pupils to go on to employment has become an integral part of school and home life. There are always going to be risks using any form of communication which lies within the public domain. Therefore, it is imperative that there are clear rules, procedures and guidelines to minimise those risks whilst pupils use these technologies.

The main areas of risk for our school community can be summarised as follows:

Content

- Exposure to inappropriate content
- Lifestyle websites promoting harmful behaviours
- Hate content
- Content validation: how to check authenticity and accuracy of online content

Contact

- Grooming (sexual exploitation, radicalisation, criminal activity etc.)
- Online bullying in all forms
- Social or commercial identity theft, including passwords

Conduct

- Aggressive behaviours (bullying)
- Privacy issues, including disclosure of personal information
- Digital footprint and online reputation
- Health and well-being (amount of time spent online, gambling, body image)
- Sexting
- Copyright (little care or consideration for intellectual property and ownership)

It is the aim and duty of Bevington to ensure that pupils, teachers, administrative staff, and visitors are protected from potential harm whilst accessing online technology on school premises.

Whilst Bevington will endeavour to safeguard and mitigate against all risks, it will never be able to completely eliminate them all. Any incidents that may come to our notice will be dealt with quickly

and according to our school policies and procedures to ensure that we continue to protect all pupils at Bevington.

The involvement of pupils and parents/carers is also vital to the successful use of online technologies. This policy also aims to inform how parents and pupils are part of the procedures, and how pupils are educated to be safe and responsible users so that they can make good judgments about information they see, find and use.

The purpose of this policy is to:

- Set out what will be taught across the three phases at Bevington (EYFS, KS1 & KS2) regarding being safe online, educating pupils about cyber bullying the consequences of such actions.
- Set out the key principles expected of all members of the school community at Bevington Primary School with respect to the use of IT-based technologies.
- Safeguard and protect all children and staff at Bevington.
- Assist school staff working with children to work safely and responsibly with the Internet and other IT and communication technologies and to monitor their own standards and practice.
- Set clear expectations of behaviour and/or codes of practice relevant to responsible use of the Internet for educational, personal or recreational use for the whole school community.
- Have clear structures to deal with online abuse such as online bullying
- Ensure that all members of the school community are aware that unlawful or unsafe behaviour is unacceptable and that, where appropriate, disciplinary or legal action will be taken.
- Minimise the risk of misplaced or malicious allegations made against adults who work with pupils.

Scope

This policy applies to all members of Bevington Primary School community (including staff, pupils, volunteers, parents/carers, visitors, community users) who have access to and are users of Bevington Primary School IT systems, both in and out of Bevington Primary School.

2. Online Safety Staff Roles and Responsibilities

Role	Key Responsibilities
Shainey Slater ***(Designated Safeguarding Lead)***	• Must be adequately trained in off-line and online safeguarding, in-line with statutory guidance and relevant Local Safeguarding Children Board (LSCB) guidance • To lead a 'safeguarding' culture, ensuring that online safety is fully integrated with whole school safeguarding. • To take overall responsibility for online safety provision • To take overall responsibility for data management and information security ensuring school's provision follows best practice in information handling • To be responsible for ensuring that all staff receive suitable training to carry out their safeguarding and online safety roles • To be aware of procedures to be followed in the event of a serious online safety incident • Ensure suitable 'risk assessments' undertaken so the curriculum meets needs of pupils, including risk of children being radicalised • To receive regular monitoring reports from the Safeguarding Co-ordinator • To ensure that there is a system in place to monitor and support staff who carry out internal online safety procedures, e.g. network manager • To ensure Governors are regularly updated on the nature and effectiveness of the school's arrangements for online safety • To ensure school website includes relevant information.
Tracey Simpson ***(Safeguarding Co-ordinator)***	• Take day to day responsibility for online safety issues and a leading role in establishing and reviewing the school's online safety policy/documents • To liaise regularly with the Computing Leader and Network Manager/Technician to discuss online safety monitoring and filtering. • To communicate regularly with SLT and the Safeguarding Governor to discuss current issues and review any incidents • To ensure that all staff are aware of the procedures that need to be followed in the event of an online safety incident • Liaise with the Local Authority and relevant agencies • Is regularly updated in online safety issues and legislation, and be aware of the potential for serious child protection concerns.
Stella Brade ***Safeguarding Governor (including online safety)***	• To review and take to the Governing body the Online Safety Policy for approval. • To approve the Online Safety Policy and review the effectiveness of the policy • To support the school in encouraging parents and the wider community to become engaged in online safety activities • To monitor school procedures and practices in Online Safety through governor monitoring visits, and meetings with key staff
Steve Smith ***(Computing Curriculum Leader)***	• To lead a 'safeguarding' culture, ensuring that online safety is fully integrated with whole school safeguarding. • To ensure the school uses appropriate IT systems and services including, filtered Internet Service, e.g. LGfL services • Promote an awareness and commitment to online safety throughout

Role	Key Responsibilities
	the school community • Ensure that online safety education is embedded within the curriculum • Liaise with school technical staff where appropriate • To ensure that online safety incidents are logged as a safeguarding incident • Facilitate training and advice for all staff • Oversee any pupil surveys / pupil feedback on online safety issues • To oversee the delivery of the online safety element of the Computing curriculum • To ensure all LGfL services are managed on behalf of the school following data handling procedures as relevant
Tariq Khodabux ***(Network Manager/Technician)***	• To monitor filtering and internet usage on the school network and report any online safety related issues to the Safeguarding Co-ordinator • To manage the school's computer systems, ensuring - school password policy is strictly adhered to. - systems are in place for misuse detection and malicious attack (e.g. keeping virus protection up to date) - access controls/encryption exist to protect personal and sensitive information held on school-owned devices - the school's policy on web filtering is applied and updated on a regular basis • That they keep up to date with the school's online safety policy and technical information in order to effectively carry out their online safety role and to inform and update others as relevant • That the use of school technology and online platforms are regularly monitored and that any misuse/attempted misuse is reported to the Safeguarding Co-ordinator/Headteacher • To ensure appropriate backup procedures and disaster recovery plans are in place • To keep up-to-date documentation of the school's online security and technical procedures
Hayley Murphy ***(Data and Information Manager)***	• To ensure that the data they manage is accurate and up-to-date • Ensure best practice in information management. i.e. have appropriate access controls in place, that data is used, transferred and deleted in-line with data protection requirements.
Stephen Smith & Shainey Slater ***(PSHE Subject Leads)***	• To plan and implement how Online Safety and cyber bullying are taught across the wider curriculum.

3. Pupils

Our pupils are:

- Involved in the review of our Acceptable Use Agreement through discussion in lessons and other forums
- Responsible for following the Acceptable Use Agreement whilst within school as agreed each academic year or whenever a new pupil starts at the school for the first time, and required to sign that they have read and understood the rules
- Taught to use the internet in a safe and responsible manner through, for example, Computing and PSHE lessons
- Taught to immediately tell an adult about any inappropriate materials or contact from someone they do not know
- Made aware of the potential use of online digital technologies to expose young people to inappropriate contact from strangers and to extremist ideas and know what to do if they encounter such issues
- Taught and encouraged to consider the implications for misusing the internet and, for example, posting inappropriate materials to websites
- Taught that the downloading of materials, for example music files and photographs, needs to be appropriate and 'fit for purpose', based on research for school work, and be copyright free
- Taught to understand what is meant by online safety through age appropriate delivery
- Taught that sending malicious or hurtful messages outside of the school can become a matter whereby the school may set sanctions or involve outside agencies such as the police
- Taught not to put themselves at risk online or through mobile phone use and taught what to do if they are concerned they have put themselves at risk
- Given explicit guidelines and procedures for using mobile phones and other personal devices in school

In the event of inappropriate use by pupils

Should a pupil be found to deliberately misuse digital or online facilities whilst at school, then appropriate sanctions will be applied, in accordance with our Behaviour Policy. If a pupil accidentally accesses inappropriate materials the pupil is expected to report this to an appropriate member of staff immediately and take action to minimize the screen or close the window. Should a pupil use the internet whilst not on the school premises in such a way as to cause hurt or harm to a member of the school community, the school will act quickly and in accordance with our Behaviour and Anti-Bullying Policies.

4. Staff

It is the responsibility of all adults within the school to:

- Be up to date with online safety knowledge appropriate for different age groups
- To ensure they are familiar with and fully support the pupil Acceptable Use Agreement
- To be vigilant when using technology as part of lessons
- To model safe and responsible use of technology
- To provide reminders and guidance to pupils on Online Safety
- Ensure that pupils are protected and supported in their use of online technologies, and that they know how to use them in a safe and responsible manner
- Not leave a computer or other device unattended whilst they are logged on
- Lock away or safely secure all portable ICT equipment when not in use
- Not to connect with any current pupil on any social networking site, or via personal mobile phones and follow the staff Code of Conduct and Acceptable Use Agreement
- Protect confidentiality and not disclose information from the network, or pass on security passwords
- Make sure that any information subject to Data Protection is not stored on unencrypted portable media or transported in an insecure form
- Protect confidentiality and not disclose information from the network, or pass on security passwords
- Use their discretion when communicating electronically about work-related issues and not bring the school's reputation into disrepute
- To use school email accounts for professional use only, and in accordance with our staff Code of Conduct
- To ensure that any personal mobile phones with school email access are protected with a passcode
- To ensure that the Network Manager is informed immediately if a mobile phone with school email access is lost or stolen
- To keep mobile phones in silent mode and completely out of sight while in an area frequented by children
- To keep mobile phones away in a locked cupboard when working in a class room or surrounding areas frequented by students
- Report any concerns about a pupil related to safeguarding and e-safety to the Designated Safeguarding Lead (DHT) or Safeguarding Co-ordinator
- Report accidental access to inappropriate materials to the Designated Safeguarding Lead /Safeguarding Coordinator so that inappropriate sites are added to the restricted list
- Only use school owned devices and memory cards to take photographs or videos, including at events and school trips and visits.

In the event of inappropriate use by staff

If a member of staff is believed to have misused the internet or network in an abusive or illegal manner from school, a report must be made to the Headteacher and/or Deputy Headteacher immediately. Safeguarding procedures must be followed to deal with any serious misuse, a report filed, and all appropriate authorities contacted as necessary.

5. Parents and Visitors

All parents have access to a copy of this Online Safety Policy on our website. Parents are asked to explain and discuss the rules with their child, where appropriate, so that they are clearly understood and accepted.

As part of the approach to developing online safety awareness with pupils, the school may offer parents the opportunity to find out more about how they can support the school to keep their child safe whilst using online technologies beyond school; this may be by offering parent education sessions or by providing advice and links to useful websites. The school wishes to promote a positive attitude to using the internet and therefore asks parents to support their child's learning and understanding of how to use online technologies safely and responsibly.

Parents should be aware that the school cannot take responsibility for a pupil's misuse or abuse of IT equipment when they are not on the school premises. This includes social networking with other pupils, and the possibility of pupils accessing inappropriate content. However, should parents or guardians become aware of an issue we strongly encourage prompt communication with the school so we can offer advice and support. The school has a duty to report serious concerns to local authority safeguarding teams or to the police, in line with statutory requirements.

Wi-Fi Access

Parents and visitors to the school are expected to abide by this policy. Should visitors wish to access the internet via the school's Wi-Fi, they will be issued with a password. Access is only permitted once they have agreed to the school's terms and conditions.

Permission for photographs and videos

If parents do not wish their child's photograph to be used on the school website or social media, we ask parents to opt-out by signing our photograph/video consent form. We do not identify individual pupils online and never use full names with photographs.

At school events (e.g. assemblies), we ask parents to refrain from taking photographs or videos, as these can be disruptive, as well as raising photographic consent issues.

6. The School's Responsibilities

The school takes its responsibilities in relation to the acceptable use of technology by pupils and adults seriously and understands the importance of monitoring, evaluating and reviewing its procedures regularly.

Filtering and Safeguarding Measures

The school's internet has a robust filtering system which is set at an appropriate level such that inappropriate content is filtered. The system logs all attempts to access the internet, including all attempts to access inappropriate content. All such attempts are reported to the Safeguarding Co-ordinator

Anti-virus, anti-spyware, junk mail and SPAM filtering is used on the school's network, stand-alone PCs, laptops and tablets, and is updated on a regular basis. Security measures are in place to ensure information about our pupils cannot be accessed by unauthorised users.

Strong encryption is used on the wireless network to provide good security.

The school's use of images and videos

The school abides by the recently revised Data Protection Act 2018 and the GDPR 2018 policy and understands that an image or video is considered personal data. Parents and Guardians may withdraw their permission at any time by informing the administration team.

Staff are not permitted to use their own devices or memory cards to record videos or photographs of pupils and when storing images within the school's network are requested to only use the pupil's first name.

The curriculum and tools for learning

The school teaches our pupils how to use the internet safely and responsibly, for researching information, exploring concepts, deepening knowledge and understanding, and communicating effectively in order to further learning, through ICT and/or PSHE lessons. The following concepts, skills and competencies are taught:

- Digital citizenship
- Future work skills
- Internet literacy
- Making good judgments about websites and emails received
- Knowledge of risks such as viruses, and opening mail from a stranger
- Access to resources that outline how to be safe and responsible when using any online technologies
- Knowledge of copyright and plagiarism issues
- file-sharing and downloading illegal content
- Uploading information – knowing what is safe to upload, and not to upload personal information
- Where to go for advice and how to report abuse

These skills are taught explicitly within the ICT curriculum but are likely to be covered in other subjects; pupils are taught skills to explore how online technologies can be used effectively, in a safe and responsible manner.

Monitoring

It is the responsibility of the Network Manager/Technician to ensure appropriate systems and technologies are in place to monitor and maintain the safeguarding and security of everyone using the school network. They monitor the use of online technologies and the use of the internet by pupils and staff, and provide at least a termly report to the Safeguarding Co-ordinator and Senior Leadership Team. Other key staff will conduct regular audits with pupils to assess their knowledge and understanding of issues related to online safety and act on any areas of vulnerability.

To audit online safety and the effectiveness of this policy, the following questions should be considered:

- Has recording of online safety incidents been effective – are records kept?
- Did the school feel able to respond effectively to any incidents?
- Were incidents resolved to the best of the school's ability?
- Do all pupils demonstrate an awareness of online safety appropriate to their age?
- Have complaints or concerns with the policy been recorded and addressed?
- Have there been significant developments in technology that should be addressed either within the curriculum or as part of staff awareness training?
- Is the policy clear to all staff and seen as appropriate and working?
- Is the current wording fit for purpose and reflective of technology use in the school?
- Do all members of the school community know how to report a problem?
- Is online safety observed in teaching and present in curriculum planning documents?

Ownership and consultation	
Document sponsor (role)	Computing Curriculum Leader
Document author (name)	Stephen Smith
Consultation	Karen Matthews, Headteacher Shainey Slater Designated Safeguarding Lead Tracey Simpson Safeguarding Coordinator Siobhan McGrath, Governor Stephen Smith, PSHE Leader

Audience	
Audience	All school based staff and volunteers

Version control	
Implementation date	September 2019
Review date	September 2020

Related documentation	All safeguarding related policies, including: o Acceptable Use Policy o Anti-Bullying and Behaviour policy o Code of Conduct o Exclusions procedures o Health and Safety Policy o PSHE Policy o Safeguarding and Child Protection Policy o Special Educational Needs Policy o Staff Discipline, Conduct and Grievance Policies o Staff Handbook o Whistleblowing Policy

Review of Policy and Procedures

Bevington carries out an annual review of this Policy, led by the Computing Curriculum Leader. This includes an evaluation of the extent to which these policies have been effectively implemented throughout the school. The Governors will remedy any deficiencies or weaknesses in child protection arrangements without delay and without waiting for the next policy review date, should any be necessary.

Appendix 1 – Procedures in the event of a breach of this policy

A An inappropriate website is accessed inadvertently

- Report website to the Safeguarding Co-ordinator or the Network Manager/Technician.
- Contact ICT Support via the Staff Shared Drive so that it can be added to the banned or restricted list.

B An inappropriate website is accessed deliberately

- Ensure that no one else can access the material, by shutting down the computer.
- Record the incident in writing on a Record of Concern Form or Behaviour Incident Form, depending on the nature of the incident
- Report to the Designated Safeguarding Lead or Headteacher, depending on the nature of the incident.
- Headteacher to refer to the Online Safety Agreement and follow agreed actions for discipline if appropriate.
- Designated Safeguarding Lead to take futher/alternative action if appropriate.

C An adult receives inappropriate material

- Do not forward this material to anyone else – doing so could be an illegal activity
- Alert the Network Manager/Technician immediately
- Ensure the device is shut down, and record the nature of the material.

D An adult has used ICT equipment inappropriately

- Follow the procedures set out in the Staff Code of Conduct and Acceptable Use Agreement.

E An adult has communicated with a pupil, or used ICT equipment, inappropriately

- Ensure the pupil is reassured
- Report to the Headteacher who should then follow the Safeguarding Policy including recording the details of the incident
- Preserve the information received by the pupil if possible, and determine whether the information received is abusive, threatening or innocent
- If illegal or inappropriate use is established, contact the Headteacher or the Chair of Governors (if allegation is made against the Headteacher) and the Designated Safeguarding Lead immediately, and follow the Safeguarding Policy.

F Threatening or malicious comments are posted online about an adult in school

- Preserve any evidence.
- Inform the Headteacher and Chair of Governors immediately and follow Safeguarding Policy and/or Behaviour Policy as necessary.

F Where images of staff or adults are posted on inappropriate websites, or have inappropriate information about them posted anywhere

- The Headteacher and Chair of Governors should be informed.

Appendix 2 – Pupil Acceptable Use Agreement

All pupils must follow the conditions described in this policy when using school ICT networked resources including: school desktop computers, iPads, cameras, Internet access, the LGFL Learning Platform both in and outside of school.

Breaking these conditions may lead to:

- Withdrawal of the pupil's access,
- Close monitoring of the pupil's network activity,
- Investigation of the pupils past network activity,
- Sanctions in accordance with our Behaviour Policy,
- In very rare and serious cases, criminal prosecution.

Pupils will be provided with guidance by staff in the use of the resources available through the school's network. School staff will regularly monitor the network to make sure that it is being used responsibly. The school will not be responsible for any loss of data as a result of the system or pupil mistakes in using the system. Use of any information obtained via the network is at the pupil's own risk.

Conditions of Use

Pupil access to the networked resources is a privilege, not a right. Pupils will be expected to use the resources for the educational purposes for which they are provided. It is the personal responsibility of every pupil to take all reasonable steps to make sure they follow the conditions set out in this Policy. Pupils must also accept personal responsibility for reporting any misuse of the network to the Network Manager.

Acceptable Use

Pupils are expected to use the network systems in a responsible manner. It is not possible to set a complete set of rules about what is, and what is not, acceptable. All use however should be consistent with the school ethos, code of conduct and the Bevington Values. Upon starting the school each pupil will sign an Acceptable Use agreement, alongside their parent/guardian. Any future changes to the Acceptable Use Agreement will be discussed with the Headteacher, Senior Leadership Team, Staff, Parents and Pupils.

A key component of the Acceptable Use Agreement is the education that pupils receive within curriculum time surrounding online safety and acceptable use of digital devices and the internet. Online safety is taught as part of Computing and PSHE.

Appendix 3 – EYFS Pupil Acceptable Use Agreement

Bevington Primary School

EYFS Pupil Acceptable Use Agreement:

- I will help to look after all digital equipment at Bevington.
- I will tell an adult if any digital equipment is broken.
- I will use only my login details.
- I will log out when my lesson/session ends.
- I will tell an adult if anything I see on a screen that worries me and use Hector the Dolphin.
- I will only go on websites that an adult has says I can access.

I can confirm I have read and understood the above statements.

NAME: _____

DATE: _____

Appendix 4 – KS1 & KS2 Pupil Acceptable Use Agreement

Bevington Primary School

KS1 & KS2 Pupil Acceptable Use Agreement:

- I will respect and look after all digital equipment at Bevington.
- I will think before I send or post a message/comment to ensure that it is kind, necessary, inspiring, helpful and true.
- I will only log in using my username and password.
- I will not share my login details (username and password) with anyone else.
- I will always log off at the end of my lesson/session.
- If I find an unattended machine logged on under another user's username I will not continuing using the machine – I will log it off immediately.
- I will not reveal any personal information (e.g. home address, telephone number) about myself or other users over the internet.
- I will use the rules of SMART when accessing the internet (Stay Safe, Not Meet Up, Accepting Files, Reliable, Tell Someone).
- If something appears on my screen that is inappropriate or worries me I will click Hector the Dolphin and tell an adult immediately.
- I will not attempt to visit websites that might be considered inappropriate or illegal. I am aware that downloading some material is illegal and the police or other authorities may be called to investigate such use.

I understand that if I don't follow the Pupil Acceptable Use Agreement I may be liable to restricted access to the school's digital devices and internet access.

I can confirm I have read and understood the above statements.

NAME: _____

DATE: _____