BEMPTON PRIMARY SCHOOL

E-Safety Policy

Date created	March 20
Created by	Mr G.Bollon
Next Review date	March 22

At Bempton Primary School we recognise that the Internet and other technologies have an important role in the learning and teaching process. The Internet is an essential element in 21st century life for education, business and social interaction. The school has a duty to provide pupils with quality Internet access as part of their learning experience. There are many benefits to using the internet both inside and outside of the classroom and, as a school, we are dedicated to the use of new technologies to enhance teaching and learning. However, we also recognise that it is equally important to balance these benefits with an awareness of the potential risks. This policy will identify how issues surrounding e safety are addressed throughout our school and will also reflect our school's commitment to the safeguarding and well-being of pupils.

Responsibilities

We believe that E-Safety is the responsibility of the whole school community, and everyone has their part to play in ensuring all members of the community are able to benefit from the opportunities that technology provides for learning and teaching. The following responsibilities demonstrate how each member of the community will contribute.

Responsibilities of the Leadership Team

- Develop and promote an E-Safety culture within the school community.
- Support the E-Safety coordinator in their work.
- Upon request make appropriate resources, training and support available to members of the school community to ensure they are able to carry out their roles with regard to E-Safety effectively.
- Receive and regularly review E-Safety incident logs and ensure that the E-Safety Coordinator follows procedures should an E-Safety incident occur in school.
- Take ultimate responsibility for the E-Safety of the school community.

Responsibilities of the E-Safety Coordinator (named person Grant Bollon)

- Promote an awareness and commitment to E-Safety throughout the school.
- Be the first point of contact in school on all E-Safety matters.
- Create and maintain E-Safety policies and procedures.
- Develop an understanding of current E-Safety issues, guidance and appropriate legislation.
- Ensure all members of staff receive an appropriate level of training in E-Safety issues
- Ensure that E-Safety education is embedded across the curriculum.

• Ensure that E-Safety is promoted to parents and carers; this can be achieved through letters, website links and formal
meetings, as regular as once a term.
• Liaise with the local authority, the local safeguarding children's board and other relevant agencies as appropriate.
• Monitor and report on E-Safety issues to Governors.
• Ensure an E-Safety incident log is kept up-to-date.

Responsibilities of Teachers and Support Staff
• Read, understand and help promote the school's E-Safety policies and guidance.
• Read, understand and adhere to the school staff AUP.
• Develop and maintain an awareness of current E-Safety issues and guidance.
• Model safe and responsible behaviours in your own use of technology.
• Teach e safety across the curriculum
• Embed E-Safety messages in learning activities where appropriate.
• Supervise pupils carefully when engaged in learning activities involving technology.
• Be aware of what to do if an E-Safety incident occurs.
• Maintain a professional level of conduct in their personal use of technology at all times (e.g. ensure you have no parents as FB friends as well as colleagues as FB friends).

Responsibilities of Technical Staff (Contracted companies- currently SMD Consultancy)
• Read, understand, contribute to and help promote the school's E-Safety policies and guidance.
• Read, understand and adhere to the school staff AUP.
• Support the school in providing a safe technical infrastructure to support learning and teaching.
• Take responsibility for the security of the school ICT system.
• Report any E-Safety-related issues that come to your attention to the E-Safety coordinator.
• Develop and maintain an awareness of current E-Safety issues, legislation and guidance relevant to your work.
• Maintain a professional level of conduct in their personal use of technology at all times.

Responsibilities of Pupils
• Read, sign, understand and adhere to the school pupil AUP.
• Help and support the school in creating E-Safety policies and practices; and adhere to any policies and practices the school creates.
• Take responsibility for learning about the benefits and risks of using the Internet and other technologies in school and at home.
• Take responsibility for your own and each others' safe and responsible use of technology in school and at home, including judging the risks posed by the personal technology owned and used by pupils outside of school.
• Ensure you respect the feelings, rights, values and intellectual property of others in your use of technology in school and at home.
• Understand what action you should take if you feel worried, uncomfortable, vulnerable or at risk whilst using technology in school and at home, or if you know of someone who this is happening to.
• Discuss E-Safety issues with family and friends in an open and honest way.

Responsibilities of Parents

• Help and support our school in promoting E-Safety.
• Be aware of and promote the school pupil AUP with your children.
• Take responsibility for learning about the benefits and risks of using the Internet and other technologies that your children use in school and at home.
• Take responsibility for their own awareness and learning in relation to the opportunities and risks posed by new and emerging technologies
• Discuss E-Safety concerns with your children, show an interest in how they are using technology, and encourage them to behave safely and responsibly when using technology.
• Model safe and responsible behaviours in your own use of technology.
• Consult with the school if you have any concerns about your children's use of technology.

Responsibilities of Governing Body

• Read, understand, contribute to and help promote the school's E-Safety policies and guidance.
• Develop an overview of the benefits and risks of the Internet and common technologies used by pupils.
• Develop an overview of how the school IT infrastructure provides safe access to the Internet.
• Develop an overview of how the school encourages pupils to adopt safe and responsible behaviours in their use of technology in and out of school.
• Support the work of the E-safety co-ordinator in promoting and ensuring safe and responsible use of technology in and out of school, including encouraging parents to become engaged in E-Safety activities.
• Ensure appropriate funding and resources are available for the school to implement their E-Safety strategy.

How parents will be involved

We believe it is important to help all our parents develop sufficient knowledge, skills and understanding to be able to help keep themselves and their children safe. To achieve this we will:

• Arrange parent training for E-Safety through a parents evening, usually in summer term or as per parents require.
• Include useful links and advice on E-Safety regularly in newsletters and on our school website.
• Provide each parent with copies of information from E safety websites e.g. ThinkUKnow.

Managing ICT Systems and Access

• Parents must sign an internet access agreement before their child/children are allowed access to the internet in school. Staff will be made aware of any children who have not been given their parents' consent.

The school will be responsible for ensuring that access to the ICT systems is as safe and secure as reasonably possible.

• Servers and other key hardware or infrastructure will be located securely with only appropriate staff permitted access.

• Servers, workstations and other hardware and software will be kept updated as appropriate.

• Virus protection is installed on all appropriate hardware, and will be kept active and up-to-date.

• The school will agree which users should and should not have Internet access, and the appropriate level of access and supervision they should receive.

• All users will agree to an end-user Acceptable Use Policy (AUP) provided by the school, appropriate to their age and access. Users will be made aware that they must take responsibility for their use of, and behaviour whilst using, the school ICT systems, and that such activity will be monitored and checked.

• In EYFS and Year 1 pupils will access the Internet using a pupil log-on, which the teacher supervises. All Internet access will be by working alongside a member of staff, or if working independently a member of staff will supervise at all times.

• Pupils will access the Internet using the pupil log on which is configured to provide appropriate filters and restrictions to internet usage.

• Internet access will always be supervised by a member of staff.

• Members of staff will access the Internet using an individual log-on, which they will keep secure. They will ensure they log-out after each session, and not allow pupils to access the Internet through their log-on. They will abide by the school's staff AUP at all times.

• Any administrator or master passwords for school ICT systems should be kept secure and available to the ICT Coordinator, Network manager and technical staff.

• We will regularly review our Internet access in light of any issues, developments requests etc.

• Staff will not attempt to access a website or conduct a search in front of pupils that hasn't been checked before the lesson.

Wireless Networking

• Our wireless network is secure and requires both an IP and network key to enable connection. These would need to be requested from a member SLT or the ICT coordinator.

Social Media

All schools, academies and local authorities have a duty of care to provide a safe learning environment for pupils and staff. Schools and local authorities could be held responsible, indirectly for acts of their employees in the course of their employment. Staff members who harass, cyberbully, discriminate on the grounds of sex, race or disability or who defame a third party may render the school or local authority liable to the injured party. Reasonable steps to prevent predictable harm must be in place.

• The school provides the following measures to ensure reasonable steps are in place to minimise risk of harm to pupils, staff and the school through limiting access to personal information:

• Training to include: acceptable use; social media risks; checking of settings; data protection; reporting issues.

• Clear reporting guidance, including responsibilities, procedures and sanctions.
• Risk assessment, including legal risk.

School staff should ensure that:
• No reference should be made in social media to pupils, parents, school staff or discussion about work
• They do not engage in online discussion on personal matters relating to members of the school community.
• Personal opinions should not be attributed to the school or local authority.
• Security settings on personal social media profiles are regularly checked to minimise risk of loss of personal information.

Filtering Internet Access
• The school uses a filtered Internet service provided by the East Riding.
• If users discover a website with inappropriate content, this should be reported to the E-Safety coordinator. This will then be blocked through contact with the East Riding internet provider.
• If users discover a website with potentially illegal content, this should be reported immediately to the E-Safety coordinator. The school will report this to appropriate agencies including the filtering provider, LA (local authority) , CEOP (child exploitation and online protection) or IWF (internet watch foundation).
• The school will regularly review the filtering and other security systems to ensure they meet the needs of all users.
• Staff can make a request for a particular website to become unblocked to the E-Safety coordinator. Access will be changed for STAFF ONLY
• Requests may be made for a website to be temporarily unblocked for the use of children E.g. if they are working on a sensitive issue in PSHCE or history. Changes to the filtering of pupil access should be logged in the safety folder with details of the date, reason the level of filtering was changed, procedures in place to deal with any incidents arising from this change and the date the website was again blocked.

Even with filters in place, it is not possible to ever provide a 100% guarantee that pupils or staff will not come across inappropriate content at all times. The school should take all reasonable steps to minimize this risk, including education and awareness and ensuring users are aware of their role in adopting safe and responsible behaviours when using the school ICT systems.

Learning and Teaching
• We will provide a series of specific E-Safety-related lessons in every year group as part of the ICT and PSCHE curriculum.
• We will celebrate and promote E-Safety through a planned programme of assemblies and whole-school activities, including promoting Safer Internet Day each year to be planned by Grant Bollon.
• We will discuss, remind or raise relevant E-Safety messages with pupils routinely wherever suitable opportunities arise during all lessons; including the need to protect personal information, consider the consequences their actions may have on others, the need to check

the accuracy and validity of information they use, and the need to respect and acknowledge ownership of digital materials.
• We will remind pupils about their responsibilities which they agreed in their AUP. This will be displayed in every classroom.
• Staff will model safe and responsible behaviour in their own use of technology during lessons.

Using Email
• Staff should use Outlook e-mail accounts allocated to them by the school, and be aware that their use of the school e-mail system will be monitored and checked.
• Communication between staff and pupils or members of the wider school community should be professional and related to school matters only.
• Any inappropriate use of the school e-mail system, or the receipt of any inappropriate messages by a user, should be reported to a member of staff immediately.

Using Images, Video and Sound
• We will remind pupils of safe and responsible behaviours when creating, using and storing digital images, video and sound. We will remind them of the risks of inappropriate use of digital images, video and sound in their online activities both at school and at home.
• Digital images, video and sound will only be created using equipment provided by the school.
• Digital images, video and sound will not be taken without the permission of participants; images and video will be of appropriate activities and participants will be in appropriate dress; full names of participants will not be used either within the resource itself, within the file-name or in accompanying text online; such resources will not be published online without the permission of the staff/pupils involved.
• All parents are invited to read and sign a Policy and Consent Form for the use of Photographs, Digital Images and Video upon entry into school. All staff will be made aware of any pupils whose parents have not given their consent. These children will be unable to have their images published online or in print.

Using Blogs, Wikis, Podcasts, Social Networking And Other Ways For Pupils To Publish Content Online
We may use blogs to publish content online to enhance the curriculum by providing learning and teaching activities that allow pupils to publish their own content. However, we will ensure that staff and pupils take part in these activities in a safe and responsible manner.
• Blogs, Wikis, Podcasts and other publishing of online content by pupils will only be used under supervision of an adult.
• Children are prohibited from using social networking sites in school.
• Where a class blog is being used, editing should be the responsibility of the staff. Any posts created by children should be done under adult supervision and approved before being published.
• If comments are used on a class blog, settings should be altered so that any comment must be approved by a member of staff before being published.
• Staff and pupils will be encouraged to adopt similar safe and responsible behaviours in their personal use of blogs, wikis, social networking sites and other online publishing outside of school.

Using Video Conferencing and Other Online Video Meetings

We may use video conferencing to enhance the curriculum by providing learning and teaching activities that allow pupils to link up with people in other locations and see and hear each other. However, we will ensure that staff and pupils take part in these opportunities in a safe and responsible manner.

• All video conferencing activity will be supervised by a suitable member of staff.

• Pupils will not operate video conferencing equipment, or answer calls, without permission from the supervising member of staff.

• Video conferencing equipment will be switched off and secured when not in use.

• Pupils will be given appropriate user rights when taking part in an online meeting room. They will not have host rights or the ability to create meeting rooms.

• Video conferencing should not take place off school premises without the permission of the head teacher.

• Parental permission will be sought before taking part in video conferences that involve people other than pupils and staff belonging to our school.

• Permission will be sought from all participants before a video conference is recorded.

• Video conferences should only be recorded where there is a valid educational purpose for reviewing the recording. Such recordings will not be made available outside of the school.

Using New Technologies

As a school we will keep abreast of new technologies and consider both the benefits for learning and teaching. Emerging technologies will be examined for educational benefit and a risk assessment will be carried out before use in school is allowed.

• We will regularly amend the E-Safety policy to reflect any new technology that we use, or to reflect the use of new technology by pupils which may cause an E-Safety risk.

Protecting Personal Data / GDPR

In order to follow GDPR guidelines and guidance staff will:

- Ensure all Ipad and laptops are locked away when not in use
- Have screens locked when not present at their devices
- Laptop passwords are changed termly
- Not save data sensitive documents on their desktops
- Ensure that no personal drives will be used with work hardware
- Make sure emails are only accessed through work devices.
- Use their supplied encrypted pen drives when storing data. The passwords for them must not be shared.

The School Website

The school website will not include the personal details, including individual e-mail addresses or full names of pupils.

• A generic contact e-mail address, managed by the Administrative staff, will be used for all enquiries or messages received electronically

• All content included on the school website and class blogs will be regularly monitored by the class teacher, ICT coordinator, Network Manager and the Head Teacher.

• The content of the website will be composed in such a way that individual pupils cannot be clearly identified.

• Staff and pupils should not post school-related content on any external website without seeking permission first.

Using Mobile Phones

The school's AUP outlines that staff usage of mobile phones is strictly prohibited, unless in the staffroom. Staff are assigned lockers to secure personal belonging including mobile phones.

The school does not allow the use of mobile phones from pupils, in school. Staff have the power to seize/confiscate mobile phones. Mobile phones can be searched if there is reasonable grounds that it contains harmful materials. The search should be conducted by the Head Teacher or a member of staff given authorisation from the Head Teacher. However if a mobile phone is being searched for sexual content then search should normally be conducted by a member of the same gender as the person being searched. However if the image being searched for is likely to be of a different gender to the person 'in possession' then the device should only be viewed by a member of the same gender as the person whose image it is. For more guidance on seizing, searching and reporting see the school's 'sexting' policy.

Dealing with E-Safety Incidents

All E-Safety incidents will be recorded on an 'Incident/disclosure form for Esafety' (Appendix 3) which will include the date, details of the incident, who was involved, who it was dealt with, how it was dealt with. This log will be kept in the E-Safety coordinators E-Safety file.

A list of incidents that may be encountered are:

• accessing illegal content deliberately
• accessing inappropriate content deliberately
• accessing illegal content accidentally and failing to report this
• accessing inappropriate content accidentally and failing to report this
• inappropriate use of personal technologies (e.g. mobile phones) at school
• accessing social networking sites, chat sites, instant messaging accounts or personal email where not allowed
• accessing other non-educational websites (e.g. gaming or shopping websites) during lesson time
• downloading or uploading files where not allowed
• sharing your username and password with others
• accessing school ICT systems with someone else's username and password
• opening, altering, deleting or otherwise accessing files or data belonging to someone else
• using school or personal equipment to send a message, or create content, that is offensive or bullying in nature
• attempting to circumvent school filtering, monitoring or other security systems
• sending messages, or creating content, that could bring the school into disrepute
• revealing the personal information (including digital images, videos and text) of others by electronic means (e.g. sending of messages, creating online content) without permission
• use of online content in such a way as to infringe copyright or which fails to acknowledge ownership (including plagiarising of online content)

You should also consider how you will deal with such E-Safety incidents if members of staff were involved. Examples of additional E-Safety incidents where staff could be involved would include:

- Transferring personal data insecurely
- Using digital communications to communicate with pupils in an inappropriate manner (for instance, using personal email accounts, personal mobile phones, or communicating via social networking sites)
- Failure to abide by copyright of licencing agreements (for instance, using online resources in lessons where permission is not given)

In most situations, where a member of staff is made aware of a possible E-Safety incident, they should inform the E-Safety coordinator, child protection coordinator / safeguarding officer or Head Teacher who will then use your school's agreed procedure to respond in the most appropriate manner.

The sanctions to be used when dealing with an e safety incident can include: temporary/permanent loss of access to the internet, involvement of parents, involvement of the Head teacher, police involvement or other outside agencies. Sanctions will be in line with the schools Behaviour and Anti-Bullying Policy and with other East Riding Policies.