E Safety and Acceptable Use Policy

Purpose of Policy

The use of technology has become a significant component of many safeguarding issues. Child sexual exploitation; radicalisation; sexual predation: technology often provides the platform that facilitates harm. An effective approach to online safety empowers a school or college to protect and educate the whole school or college community in their use of technology and establishes mechanisms to identify, intervene in, and escalate any incident where appropriate.

Rationale

The purpose of this policy is to:
· Set out the key principles expected of all members of the school community at Baydon CE Primary School with respect to the use of computing-based technologies.
· Safeguard and protect the children and staff and comply with GDPR (General Data Protection Regulation)
· Assist school staff working with children to work safely and responsibly with the internet and other 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
· Have clear structures to deal with online abuse such as cyberbullying which are cross referenced with other school policies
· 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 student
Computing in the 21st Century is an essential resource to support learning and teaching, as well as playing an important role in the everyday lives of children, young people and adults. Consequently, we need to build in the use of these technologies to arm our young people with the skills to access lifelong learning and employment. Computing covers a wide range of resources including; web-based and mobile learning. It is also important to recognise the constant and fast paced evolution of computing within our society.
Currently the internet technologies children and young people are using both inside and outside of the classroom include:
• Websites/ Learning Platforms and Virtual Learning Environments
• Email and Instant Messaging
• Chat Rooms and Social Networking
• Blogs
• Podcasting
• Video Broadcasting

• Music Downloading
• Gaming
• Mobile/ Smart phones/ other mobile devices with text, video and/ or web functionality

Whilst exciting and beneficial both in and out of the context of education, much ICT, particularly web based resources, are not consistently policed. All users need to be aware of the range of risks associated with the use of these Internet technologies. The breadth of issues classified within online safety is considerable, but can be categorised into four areas of risk: content, contact, conduct and commerce (KCSiE 2021) The main areas of risk are as follows:

• **content:** being exposed to illegal, inappropriate or harmful content, for example: pornography, fake news, racism, misogyny, self-harm, suicide, anti-Semitism, radicalisation and extremism.
• **contact:** being subjected to harmful online interaction with other users; for example: peer to peer pressure, commercial advertising and adults posing as children or young adults with the intention to groom or exploit them for sexual, criminal, financial or other purposes'.
• **conduct:** personal online behaviour that increases the likelihood of, or causes, harm; for example, making, sending and receiving explicit images (e.g consensual and non-consensual sharing of nudes and semi-nudes and/or pornography, sharing other explicit images and online bullying; and
• **commerce** - risks such as online gambling, inappropriate advertising, phishing and or financial scams.

Roles and Responsibilities

Communicating the policy

• Policy to be posted on the school website/ staffroom.
• Policy to be part of school induction pack for new staff.
• Acceptable use agreements discussed with pupils at the start of each year.

Handling Complaints
The school will take all reasonable precautions to ensure that users access only appropriate material. (See Management of the filtering system). However, due to the global and connected nature of Internet content, it is not possible to guarantee that access to unsuitable material will never occur via a school computer. The school can not accept liability for the material accessed, or any consequences resulting from Internet use.
Complaints of Internet misuse (including social networking concerns) will be dealt with by a senior member of staff. Our Head teacher acts as first point of contact for any e-safety complaint.
Complaints of cyberbullying are dealt with in accordance with our Anti-bullying Policy.
Complaints related to child protection are dealt with in accordance with school / LA child protection procedures.
Pupils and parents will be informed of the complaints procedure. Parents and pupils will need to work in partnership with staff to resolve issues.

Sanctions may include:
A temporary or permanent ban on Internet use.
Suspension of online learning site logins
Additional disciplinary action may be added in line with the school's behaviour policy.
Where applicable, parents and other external agencies may be contacted.

Review and monitoring

The e-safety policy is referenced from within other school policies: Child Protection policy, Anti-Bullying policy, Behaviour policy, Personal, Social and Health Education Policy, and in the Remote Education Provision document.
The school has a Designated Safeguarding Lead- DSL who will be responsible for document ownership, review and updates. The e-safety policy will be reviewed bi-annually or when any significant changes occur regarding the technologies in use within the school.
The e-safety policy has been written by the school DSL and is current and appropriate for its intended audience and purpose.
There is widespread ownership of the policy and it has been agreed by the SLT and approved by the Governing Body. All amendments to the school e- safety policy will be discussed in detail with all members of teaching staff.

Education and Curriculum

Internet use to benefit education

The purpose of Internet use in school is to raise educational standards, to promote pupil achievement, to support the professional work of staff and to enhance the school's management functions. Internet use is part of the statutory curriculum and a necessary tool for learning. Internet access is an entitlement for pupils who show a responsible and mature approach to its use. 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. Pupils use the Internet widely outside school and will need to learn how to evaluate Internet information and to take care of their own safety and security.

Benefits of using the Internet in education include:

- access to world-wide educational resources including museums and art galleries;
- educational and cultural exchanges between pupils world-wide;
- vocational, social and leisure use in libraries, clubs and at home;
- access to experts in many fields for pupils and staff;
- professional development for staff through access to national developments,
- educational materials and effective curriculum practice;
- collaboration across support services and professional associations;
- improved access to technical support including remote management of networks and automatic system updates;
- exchange of curriculum and administration data with Wiltshire County Council and DfE;
- access to learning wherever and whenever convenient

The school Internet access will be designed expressly for pupil use and will include filtering appropriate to the age of pupils. Pupils will be taught what Internet use is acceptable and what is not and given clear objectives for Internet use. Internet access will be planned to enrich and extend learning activities. Access levels will be reviewed to reflect the curriculum requirements and age of pupils. Staff should guide pupils in on-line activities that will support the learning outcomes planned for the pupils' age and maturity. Pupils will be educated in the effective use of the Internet in research, including the skills of knowledge location, retrieval and evaluation. At Key Stage 1, access to the Internet will be by adult demonstration and directly supervised access to specific, approved on-line materials.

Pupil e-safety curriculum

From September 2020 schools must have regard to the new statutory guidance for teaching about online relationships. The guidance explains the significant role the internet plays in pupils' lives.

Baydon CE Primary School has a clear, progressive e-safety education programme as part of the PSHE curriculum and the Computing curriculum. While progressing through the PSHE curriculum pupils will study specific units regarding e-safety (digital wellbeing). However, online safety is a running and interrelated theme throughout all studies and is referred to throughout all areas as frequently as possible.

Our ongoing education for pupils covers a range of skills and behaviours appropriate to their age and experience, including:

to develop a range of strategies to evaluate and verify information before accepting its accuracy;

to be aware that the author of a web site / page may have a particular bias or purpose and
to develop skills to recognise what that may be;
to know how to narrow down or refine a search;
[for older pupils] to understand how search engines work and to understand that this affects the results they see at the top of the listings;
to understand acceptable behaviour when using an online environment / email, i.e. be polite, no bad or abusive language or other inappropriate behaviour; keeping personal information private;
to understand how photographs can be manipulated and how web content can attract the wrong sort of attention;
to understand why on-line 'friends' may not be who they say they are and to understand why they should be careful in online environments; o to understand why they should not post or share detailed accounts of their personal lives, contact information, daily routines, location, photographs and videos and to know how to ensure they have turned-on privacy settings;
to understand why they must not post photos or videos of others without their permission;
to know not to download any files – such as music files - without permission;
to have strategies for dealing with receipt of inappropriate materials;
to have an age appropriate understanding of the impact of cyberbullying, sexting and trolling and know how to seek help if they are affected by any form of online bullying.
to know how to report any abuse including cyberbullying; and how to seek help if they experience problems when using the internet and related technologies, i.e. parent or carer, teacher or trusted staff member, or an organisation such as ChildLine
to ensure that when copying materials from the web, they understand issues around plagiarism
to respect and acknowledge copyright / intellectual property rights
To ensure age appropriate understanding of the issues around aspects of the commercial use of the Internet. This may include risks in popups, buying on-line or on-line gaming

E-Safety rules are posted in rooms with Internet access and e-safety information is displayed in a prominent place in school. E-safety rules are revisited annually, to raise the awareness and importance of safe and responsible internet use both in school and at home

It is ensured that the copying and subsequent use of Internet derived materials by staff and pupils complies with copyright law. Pupils should be taught to be critically aware of the materials they read and shown how to validate information before accepting its accuracy. Pupils will be taught to acknowledge the source of information used and to respect copyright when using Internet material in their own work. The evaluation of on-line materials is a part of every subject.

Prevent Duty

This school takes seriously its duty contained in the Counter Terrorism and Security Act (2015) to prevent pupils and those working in school from being radicalised or drawn into extremism. We will follow the advice contained within the new statutory guidance on the legal duty set out in the Prevent Duty Guidance: For England and Wales (2015) in conjunction with the other duties which we already have for keeping pupils safe.

Managing Information Systems

Security of Information System
The security of the school information systems will be reviewed regularly. Virus protection will be updated regularly. Portable media, i.e. pen sticks, CDR and DVDs, may not be used without specific permission followed by a virus check. Sensitive data must not be removed from school via portable memory device. Unapproved system utilities and executable files will not be allowed in pupils' work areas or attached to e-mail.

Management of Published Content
The contact details on the website are the school address, school e-mail addresses and telephone number. Staff, governors or pupils' personal information must not be published. E-mail addresses should be published carefully, to avoid spam harvesting. The head teacher will take overall editorial responsibility of the website and ensure that content is accurate and appropriate.
The website should comply with the school's GDPR policy. Pupils' full names will not be used anywhere on the website, particularly in association with photographs and written permission from parents or carers must be obtained before images of pupils are electronically published.

Management of social networking and personal publishing
The schools will block/filter access to social networking sites and Newsgroups.
Pupils will be advised that when using these sites from home they should never give out personal details of any kind which may identify them and / or their location. Examples would include real name, address, mobile or landline phone numbers, school attended, e-mail addresses, full names of friends, specific interests and clubs etc.
Pupils should be advised not to place personal photos on any social network space. Advice should be given regarding background detail in a photograph which could identify the pupil or his/her location e.g. house number, street name or school.
Pupils should be advised on security and encouraged to set passwords, deny access to unknown individuals and instructed how to block unwanted communications. Pupils should be encouraged to invite known friends only and deny access to others.
Pupils should be advised not to publish specific and detailed private thoughts or actions.
Schools should be aware that bullying can take place through social networking especially when a space has been setup without a password and others are invited to see the bully's comments.

Management of the filtering system
The school will work with SWGFL and the Local Authority to ensure that systems to protect pupils are reviewed and improved. If staff or pupils discover unsuitable sites, the URL must be reported to the Computing Coordinator who will take appropriate action. Senior staff will ensure that regular checks are made to ensure that the filtering methods selected are appropriate, effective and reasonable. Any material that the school believes is illegal must be reported to appropriate agencies such as IWF or CEOP. Baydon School can request the blocking and unblocking of certain sites. Any request to unblock will be reviewed by the headteacher before completion.

Protection of Personal Data
Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 1998 and from May 2018 according to the General Data Protection Regulation (GDPR). The school will maintain a current record of all staff, governors and pupils who are granted access to the school's electronic communications.

Use of digital images
When using digital images, staff should inform and educate pupils about the risks associated with the taking, use, sharing, publication and distribution of images. In particular they should recognise the risks attached to publishing their own images on the internet e.g. on social networking sites.
• In accordance with guidance from the Information Commissioner's Office, parents / carers are welcome to take videos and digital images of their children at school events for their own personal use. To respect everyone's privacy and in some cases protection, these images should not be published or made publicly available on social networking sites, nor should parents / carers comment on any activities involving staff or other pupils in the digital / video images.
• Staff and volunteers are allowed to take digital / video images to support educational aims with permission from parents, but must follow school policies concerning the sharing, distribution and publication of those images. Those images should only be taken on school approved equipment, other equipment of staff or volunteers should not be used for such purposes.
• Care should be taken when taking digital / video images that pupils are appropriately dressed and are not participating in activities that might bring the individuals or the school into disrepute.
• Pupils must not take, use, share, publish or distribute images of others without their permission.
• Photographs published on the website, or elsewhere that include pupils will be selected carefully and will comply with good practice guidance on the use of such images.
• Pupils' full names will not be used anywhere on a website or blog, particularly in association with photographs.
• Written permission from parents or carers will be obtained upon entry to school before photographs of pupils are published on the school website or on social media.
• Pupil's work can only be published with the permission of the pupil and parents or carers.

Passwords and Emails
· This school makes it clear that staff and pupils must always keep their password private, must not share it with others and must not leave it where others can find.
· All staff have their own unique username to access school systems. Staff are responsible for keeping their password private.

· We require staff to use STRONG passwords to enter our MIS systems
· All staff to adhere to school's email protocol and email use

Equipment and Digital Content

School Mobile Devices such as ipads and laptops are used on the school network. Mobile phones brought into school are entirely at the staff member, students & parents' or visitors own risk. The School accepts no responsibility for the loss, theft or damage of any phone or hand-held device brought into school. Parents/carers/visitors are not permitted to use their mobile phones/take pictures and/or videos of staff and/or pupils on the school premises.

Student mobile phones, MP3 players, iPads, smart watches which are brought into school must be turned off (not placed on silent) and handed in to the class teacher on arrival at school. They must remain turned off and are stored in the School Office. All visitors are requested to keep their phones on silent. All mobile phone use is to be open to scrutiny and the head teacher is to be able to withdraw or restricted authorisation for use at any time if it is to be deemed necessary.

The School reserves the right to search the content of any mobile or handheld devices on the school premises where there is a reasonable suspicion that it may contain undesirable material, including those which promote pornography, violence or bullying. Where parents or students need to contact each other during the school day, they should do so only through the School's telephone.

Staff may use their phones during break times. If a staff member is expecting a personal call they may leave their phone with the school office to answer on their behalf, or seek specific permissions to use their phone at other than their break times. They should be switched off or in silent mode. Mobile phones and personally-owned mobile devices brought in to school are the responsibility of the device owner. The school accepts no responsibility for the loss, theft or damage of personally-owned mobile phones or mobile devices.

Mobile phones and personally-owned devices are not permitted to be used in certain areas within the school site, e.g. changing rooms and toilets.

Asset Disposal

Details of all school-owned hardware will be recorded in a hardware inventory. Details of all school-owned software will be recorded in a software 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 forensically wiped. Alternatively, if the storage media has failed, it will be physically destroyed.

Appendix 1

Baydon St Nicholas CE VA Primary School - Acceptable Use of ICT Agreement for Staff, Governor and any Visitors who may use any ICT equipment, technology or mobile devices whilst on school premises.

Acceptable Use Agreement / Code of Conduct

ICT and the related technologies such as email, the internet and mobile devices are an expected part of our daily working life in school. This policy is designed to ensure that all staff, governors or visitors are aware of their professional responsibilities when using any form of ICT. All staff, governors or visitors are expected to sign this policy and adhere at all times to its contents. Any concerns or clarification should be discussed with the school computing co-ordinator or DSL

I will only use the school's email / Internet / Intranet / Learning Platform and any related technologies for professional purposes or for uses deemed 'reasonable' by the Head or Governing Body.

I will comply with the ICT system security and not disclose any passwords provided to me by the school or other related authorities.

I will ensure that all electronic communications with pupils and staff are compatible with my professional role.

I will not give out my own personal details, such as mobile phone number and personal email address, to pupils.

I will only use the approved, secure email system(s) for any school business (staff members only).

I will ensure that personal data (such as data held on SIMS) is kept secure and is used appropriately, whether in school, taken off the school premises or accessed remotely. Personal data can only be taken out of school or accessed remotely when authorised by the Head or Governing Body.

I will not use or install any hardware or software without permission from the ICT subject leader and in reference to St Helens ICT Services/

I will not browse, download, upload or distribute any material that could be considered offensive, illegal or discriminatory.

Images of pupils and/ or staff will only be taken, stored and used for professional purposes inline with school policy and with written consent of the parent, carer or staff member. Images will not be distributed outside the school network without the permission of the parent/ carer, member of staff or Head teacher.

I understand that all my use of the Internet and other related technologies can be monitored and logged and can be made available, on request by the Head teacher.

I will respect copyright and intellectual property rights.

I will ensure that my online activity, both in school and outside school, will not bring my professional role into disrepute.

I will support and promote the school's E-Safety Policy and help pupils to be safe and responsible in their use of ICT and related technologies.

I will ensure that only children whose parents have given permission for them to use the Internet and ICT are enabled to do so at school.

I agree to follow this code of conduct and to support the safe use of ICT throughout the school

Signature …….…… Date ……

Full Name …….....

Appendix 2

COMPUTER RULES – TO KEEP ME SAFE- KS1

I only use the internet when an adult is with me.
I only click on links and buttons when I know what they do.I keep my personal information and passwords safe online.
I only send messages online which are polite and friendly.
I know the school can see what I am doing online.
I know that if I do not follow the rules then I might be stopped using the iPads and computers in school.
I always tell an adult/teacher if something online makes me feel unhappy or worried.

Appendix 3

COMPUTER RULES – TO KEEP ME SAFE- KS2

These rules have been written to make sure that you stay safe and act responsibly when using the computers. When we talk about ICT, we are talking about computers, laptops, netbooks, and everything including cameras, web cams, I-Pads and tablets. These rules will have been discussed in class.

If you have any questions, please ask your teacher.

Keeping Safe

I will not use ICT in school without permission from my teacher

I will be careful when going on the internet. I will log off sites when I have finished

I must keep my personal details and those of others private

At all times, I will think before I click (especially when deleting or printing)

I know that teachers can, and will, check the files and websites that I have used

I will keep my usernames and passwords secure, but I understand that I can share them with appropriate people, such as my parents or teachers

Communicating

When communicating online (in blogs, emails, forums etc) I will think about the words that I use and will not use words that may offend other people. I know that I need to be polite and friendly online

I am careful about what I send as messages

When communicating online I will only use my first name and not share personal details such as my email address, address or phone number

I understand that people online might not be who they say they are

If an online friend wants to meet me I will tell an adult. I will NEVER arrange to meet anyone without permission.

Research and Fun

When using the internet, I will think about the websites that I am accessing and use the list of websites given me by my teacher

I will use clear search words so that I find the right information

When using information or pictures from websites, I will try and say which website it came from and if possible link back to the site

Sharing

I will not look at other people's files or documents without their permission

I will not install any software or hardware (including memory sticks) or try to change computer settings without permission from the teacher

I will not take or share pictures of anyone without their permission

I know that anything I put up on the internet can be read by anyone

Problems

If I find a website, image or message that is inappropriate, I will tell my teacher straight away

I will take care when using the computers and transporting equipment around. I will tell a teacher if equipment is broken or not working

I understand that if I am acting inappropriately then my parents may be informed.