Bentley CE Primary School Acceptable use Policy (E-Safety policy)

Review date	January 2026
Period of review	3 years
Next review due:	January 2029
Governor Committee	Full Governing Body

Overview

E-Safety encompasses both Internet technologies and electronic communications, such as mobile phones, as well as collaboration tools, on-line learning platforms and personal publishing. It highlights the need to educate pupils about the benefits and risks of using technology and provides safeguards and awareness for users to enable them to control their online experience.
Our e-Safety Policy has been written by the school, with government guidance.
The school's e-Safety policy will operate in conjunction with other policies including those for Computing, Behaviour, Anti-bullying, Curriculum, Child Protection, Data Protection and Security.
The school's E-Safety Co-ordinator is Zoe Hastie, the Computing Leader.

Teaching and Learning

Why Internet use is important

The Internet is an essential element in 21st century life for education, business and social interaction. The school has a duty to provide students with quality Internet access as part of their learning experience. Benefits include: access to world-wide resources and research materials, educational and cultural exchanges between pupils world-wide, access to experts in many fields, staff professional development (such as access to online learning and forums), communication with support services, professional associations and colleagues and the exchange of curricular and administration data.

The statutory curriculum requires pupils to learn how to locate, retrieve and exchange information using ICT. Consequently, in delivering the curriculum teachers need to plan to integrate the use of ICT and web-based resources including e-mail to enrich learning activities. Effective internet use is an essential life skill.

Access to the school's ICT network and use of ICT facilities owned by the school, including access to the Internet, are conditional on observance of the following Acceptable Use Policy.

The aims of this Acceptable Use Policy are to:-

- Allow all users safe access to school ICT resources and use of the Internet for educational purposes.
- Provide a mechanism by which staff and pupils are protected from Internet sites, information and individuals that would undermine the principles and aims of the school.
- Provide rules which are consistent and in agreement with the Data Protection Act 1984, Computer Misuse act 1990 and other legislation relevant to the use of computers and electronic data in schools.

- Provide rules that are consistent with the acceptable procedures commonly used on the Internet, including those associated with 'netiquette'.
- Provide rules relating to the use of computers and ICT facilities in school, which are consistent with the general policies of the school.

General Internet use and Consent

Pupils who are to have basic access to the Internet must understand the basic conventions and navigation techniques before going online and accessing material.

Pupils must have returned a signed consent form before being allowed to use the ICT facilities that involve accessing the internet. The school will keep a record which will be regularly referred to by teachers and monitored by the Headteacher and admin staff. The use of the names of pupils or photographs of pupils for websites will require written permission from parents/guardians included on the consent form. If a picture is placed on the website the child's full name will not be displayed.

Pupils must not use the school ICT facilities without their supervision of a member of staff. Although use of the ICT facilities and access to the Internet will be supervised, and all possible measures will be taken Bentley CE Primary School and the school's Internet Provider cannot accept liability for the accessing of inappropriate materials or any consequences of internet access.

Bentley CE Primary School is protected by a flexible filtering system through our Internet Service Provider, which is approved by Hampshire County Council.

If staff or pupils discover unsuitable sites, the URL (address) and content must be reported to the Computing Leader who will record the address and report to the Headteacher and Internet Service Provider.

Pupils are aware that they must only access those services they have been given permission to use.

Staff and pupils are made aware that the use of computer systems without permission or for inappropriate purposes is a criminal offence under the Computer Misuse Act 1990.

Staff and Governors must agree to and sign the Acceptable Use Agreement (Code of Conduct) each year.

Pupils will be taught how to evaluate Internet content

The school will ensure that the 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.

Managing Internet Access

Log in and Passwords

Pupils and staff must not disclose any password or login name given to anyone, or allow anyone else to use a personal account.

Pupils and staff must not attempt to gain access to the school network or any Internet resource by using someone else's account name or password.
Staff and pupils must ensure terminals or laptops are logged off or locked when left unattended.

Adult users are expected to be in charge of their own areas on the network. Passwords are therefore set for each user. Passwords should be changed regularly. Passwords should be over 4 characters and should contain letters, numbers and symbols. They should not contain spaces. Remember – passwords are case sensitive. "PASSWORD" is different to "password". Protect your work area do not tell anyone your password. Anyone who needs assistance in changing their password should contact the Computing Leader.

Artificial Intelligence (AI) and Emerging Technologies
Artificial Intelligence (AI) tools (such as text generators, image generators, chatbots and automated assistants) are becoming increasingly common in everyday life and may be encountered by pupils both in and out of school.
Bentley CE Primary School recognises the potential educational benefits of AI when used appropriately, ethically and safely, alongside the risks associated with misinformation, bias, privacy and over-reliance on technology.
The following principles apply:

- AI tools may only be used in school under the direction and supervision of a member of staff.
- Pupils are not permitted to independently access AI tools unless explicitly authorised and supervised by staff for a specific learning purpose.
- AI must not replace pupils' own thinking, creativity or learning. Work submitted by pupils must reflect their own understanding and effort.
- Pupils will be taught age-appropriate awareness that:
    - AI can make mistakes or provide inaccurate information
    - AI content may reflect bias
    - Information generated by AI should always be checked and evaluated
- Pupils must not input personal data (their own or others') into AI tools, including names, images, addresses, or any identifying information.
- AI tools must not be used to generate or access inappropriate, offensive or harmful content.
- Any use of AI must comply with:
    - Data Protection legislation
    - Safeguarding expectations
    - Copyright and intellectual property law

Staff use of AI tools must:

- Be professional, transparent and in line with school policies
- Never involve uploading or sharing pupil data or images
- Be used to support planning, administration or learning design rather than replace professional judgement
- Be declared to the Computing Leader or Headteacher where new tools are trialled

The school will regularly review its approach to AI in line with national guidance and technological developments.

Learning Platform (VLE-Virtual Learning Environment)

Bentley CE Primary School uses 'Seesaw' as VLE or Learning Platform. Activities and announcements can be assigned and feedback given when children complete tasks. Seesaw is used for homework tasks especially, but also to gain experience in its uses should we need to rely on it again for remote learning provision. All pupils have access to the VLE to create, store and update their learning. All pupils are given a log on and passwords which are shared with their parents for safe access at home.

General Safety and Risk Assessment

The consumption of food or drink is forbidden whilst using a computer. It is hazardous to the equipment and to individuals. Users must treat with respect equipment and services in school and at other sites accessed through school facilities. Malicious action will result in immediate suspension from use of the school facilities. Staff are responsible for sharing safety issues regarding use of netbooks with their pupils.

Cyber Bullying (See Anti Cyber Bullying Policy)

The experience of being cyber bullied can be very painful for those who are the targets. Adults need to help children and young people prepare for the hazards of using technology while promoting learning and social opportunities. Some forms of cyber bullying are different from other forms:

- Through a range of media children can be cyber bullied 24 hours a day.
- People who cyber bully may attempt to remain anonymous.
- Anyone of any age can cyber bully.
- Some instances of cyber bullying may be unintentional – such as text sent as a joke or an email to the wrong recipient.

We recognise that the best way to deal with cyber bullying is to prevent it from happening in the first place. By embedding good, safe ICT practice into all our teaching and learning, incidents can be avoided. We recognise we have a shared responsibility to prevent incidents of cyber bullying but the Headteacher has the responsibility for co-ordinating and monitoring the implementation of anti-cyber bullying strategies.

Understanding Cyber Bullying

The school community is aware of the definition of cyber bullying and the impact cyber bullying has. Staff receive guidance and review the Anti-Bullying and Acceptable Use Policies annually. Children are taught how to recognise cyber bullying and their responsibilities to use ICT safely. ICT is integral to teaching and learning practice in the school. Parents are also taught how to recognise cyber bullying and their responsibilities for supporting safe ICT use. The school runs regular parental updates on E-Safety via the Newsletter and workshops periodically.

Record Keeping and Monitoring Safe Practice.

As with other forms of bullying the Headteacher keeps records of any cyber bullying incidents. Incidents of cyber bullying will be followed up using the same procedures as other forms of bullying. We monitor for any misuse of school equipment and systems.

E-Safety

Children and staff are updated of E-Safety Codes of Conduct at the start of each academic year. Parents/staff are regularly offered e-Safety sessions which will be led by a trained member of staff, in this instance the Computing Leader/E-Safety Manager, or other Agencies coming in to school.

Any work or activity on the Internet must be directly related to schoolwork. Private use of the Internet (including social networking sites) in school is forbidden.

Staff who use social networking sites are reminded of the necessity to keep their profiles secure and to avoid contact with persons related to the school. Staff are reminded that any action or comment that brings the school or colleagues into disrepute or compromises pupil or staff confidentiality will be classed as a disciplinary matter.

Do not give personal email or postal addresses, telephone numbers of any teachers or pupils at the school.

Distribution of computer viruses, electronic chain mail, computer games, use of Internet Relay Chat and similar services are strictly forbidden by pupils and staff as they can result in degradation of service for other users and increase the workload of the IT technicians or staff. Do not download, use or upload any material that is copyright. Always seek permission from the owner before using any materials from the Internet. If in doubt, or you cannot obtain permission, do not use the material. Users should assume that ALL software is subject to copyright restrictions, including shareware. Pupils must not under any circumstances download or attempt to install any software on the school computers. Staff should seek the advice of the Computing Leader before attempting to download or upload software.

Under no circumstances should users view, upload or download any material that is likely to be unsuitable for children or schools. This applies to any material or violent, dangerous, racist or inappropriate sexual content. If users are unsure about this, or any materials, users must ask the Headteacher or Computing Leader. If in doubt, DO NOT USE. The transmission, storage, promotion or display of offensive, defamatory or harassing material is strictly forbidden as they breach laws of the UK under the Computer Misuse Act. Possession of certain types of unsuitable material can lead to prosecution by the police.

Search engines are not to be used to search for websites or images unless the learning objective specifically demands it.

School Network and Pupil Files

Always respect the privacy of files or other users. Do not enter the file areas of other users without their permission. Files to be shared should be saved to the Teacher or Student Shares area. Pupils can access and save work to their own log-on through the server; this must only be accessed by the child and the Computing Leader and Technicians.

Do not modify or delete the files of other users on the Teacher's drive without obtaining permission from them.

The Computing Leader and Technicians are able to view any material pupils store on the school's computers.

Users should regularly clear out their online files, removing any unwanted old files as storage space on the server is limited.

Users accessing software of any services available through school facilities must comply with licence agreements or contracts relating to their use and must not alter or remove copyright statements. Some items are licensed for educational or restricted use only.

Be polite and appreciate that other users are entitled to differing viewpoints. The use of strong language, swearing or aggressive behaviour is forbidden.

This Acceptable Use Agreement applies when using 'Busy Things', 'Times Tables Rockstars', 'Seesaw', 'Arithmagicians' and any other prescribed platforms at home.

Storage devices from home are generally not allowed, in order to prevent potential spread of viruses. Under some circumstances (for example specialist teachers visiting the school), permission to use storage devices may be granted by the Computing Leader or Headteacher. In such cases, the school's anti-virus software must be run before any files are opened or transferred. Adding any peripheral will cause a prompt to scan the device.

Security Guidelines

Backup:

Files stored on the network are backed up by our Technical Support Services on a regular basis, to enable data to be retrieved should local copies be corrupted.

Save Regularly

It is very important to save work regularly. The network is very reliable but problems do occur. If work is saved regularly and a PC or the network does fail for any reason, only the work done since the last save will be lost. Documents do not have autosave to ensure staff and pupils are aware of what is being saved and to help protect accidental overriding of documents.

Documents within the school do not operate with an automatic save function. This ensures that users are fully aware of when and what information is being saved, encouraging deliberate review before saving to reduce the risk of accidental overwriting of documents.

Use your Network Area

Always ensure that files are saved to your network area and not on the local hard drive. This will ensure that all files are backed up and can be retrieved in the event of a hardware failure or theft.

Home Documents

The school cannot accept responsibility for personal documents held on school laptops. It is the responsibility of the user to backup documents created at home.

Off-site pupil data and pupil information

Laptops and back-ups may be taken off site. Staff are to ensure that laptops are used cautiously when viewing pupil information/data and images and that laptops are logged off when left unattended. It is the responsibility of each member of staff to ensure that property taken off-site is secure and safe from theft or unauthorised use.

Virus Checks

All computers in school have anti-virus software, although very new viruses may not be found. If you suspect a virus please report to the Computing Leader straight away and report your concerns to AgileICT through their on-line support system.

Email Usage

Use of e-mail and communication by email should be treated with the same degree of care you would take if you wrote a letter to the person you are contacting. It cannot be regarded as purely private, only to be seen by the receiver. E-mail can be stored, forwarded and distributed to large numbers of people at the touch of a button. It is easy to forget that it is a permanent form of written communication and that material can be recovered even if seen to be deleted from the computer.

When using e-mail, pupils and staff should:

- Not access personal emails in school using school equipment.
- The use of school e-mail addresses for contacting parents is acceptable, whereas the use of a personal (domestic) e-mail account is prohibited. Alternatively, staff may choose to ask Office Staff to send e-mail communications on their behalf.
- Be aware that e-mail is not a secure form of communication and therefore pupils should not send any personal information.
- Must not forward e-mail messages onto others unless the sender's permission is obtained first.
- Must not open e-mail attachments from unknown senders or from computers from which virus protection may not be current or activated.
- Not send email messages in the heat of the moment and avoid writing anything that may be construed as defamatory, discriminatory, derogatory, rude or offensive.
- Must not open email attachments from unknown senders or from computers from which virus protection may not be current or activated.

This guidance will apply to any inter-computer transaction, be it through web services, chat room, bulletin and peer to peer sharing.

Mobile Devices

Pupils are generally not permitted to bring mobile phones or devices into school. Should there be the need for a child to bring their device into school, this should be turned off and handed to the class teacher until the end of the day.

Pupils may not make personal calls from a mobile phone during the school day.

Mobile phones may not be used to take pictures or videos of pupils and staff.

Pupils should not send/receive email or text messages to/from their mobile device during the school day.

Any inappropriate use of mobile devices such as cyber bullying must be reported to the Headteacher, DSL or E-Safety Co-ordinator.

Staff should only use their mobile phones at appropriate times of the day, during the school day their mobiles should be turned off or set to silent. Staff may use personal devices to take photographs, or upload a child's work to Seesaw, for example, on the understanding that any such images are removed immediately after use.

Any pupil who is seen with a mobile device during the school day will have their phone removed from them to be collected at the end of the day. The device will be kept in the school safe.

Communications

E-Safety rules will be posted in all networked rooms with Internet access and discussed with the pupils at the start of each year.

Pupils will be informed that network and Internet use will be monitored.

All staff will be asked to read, sign and return the Acceptable Use Agreement (Code of Conduct).
Staff should be aware that Internet traffic can be monitored and traced to the individual user. Discretion and professional conduct is essential at all times.

Staff training in safe and responsible Internet use and on E-Safety will be provided as required.

Legal Requirements

Users must agree to comply with all software license agreements. Do not attempt to copy any software from, or by using school computers. If you have any requirements for using additional software for any reason, please contact the Computing Leader to discuss the situation. Solutions are *usually* possible! Remember also that shareware is not freeware and must be licensed for continued use.

Computer facilities shall not be used to hold or process personal data except in accordance with the provisions of the Data Protection Act 1984. Any person wishing to use the facilities for such a purpose is required to inform the Head teacher in advance and comply with any

restrictions that the school or the UK Data Protection Registrar may impose concerning the manner in which data may be held or processed.

Copyright Designs & Patents Act - Copyright is infringed if a person acquires an unauthorised copy of a computer program. Mere acquisition, without regard to the actual or intended use, constitutes an infringement of the author's copyright. "Acquisition" includes loading a copy of a programme into the random access memory, or other temporary storage device, of a computer, or onto any form of permanent data storage medium.

The high cost of commercially marketed software and the ease with which it can be copied make it tempting to copy software illegally. Agents for software developers are aggressively seeking to protect their rights under the law. Schools can be audited at any time. Anyone found to have unauthorised copies of software will immediately be suspended from using the ICT facilities. The matter will be investigated and the necessary action taken, the school will not accept any liability whatsoever.

"Hacking" is illegal under the Computer Misuse Act 1990. Regulations regarding unauthorised access or misuse of computing facilities are enforceable under the law, any person found attempting to or hacking the school network will be prosecuted.

Regulations regarding the transmission, storage or display of obscene material are enforceable by law under the Criminal Justice and Public Order Act 1984 which amends the Obscene Publications Act 1956, the Protection of Children Act 1978 and the Telecommunications Act 1984 to extend their provisions to transmission over a data communications network.

Sanctions

If pupils break the rules as laid down by this policy they will lose temporary or permanent use of the school systems. Parents will be informed and if the law has been broken the police will be informed and the school will assist the police with any prosecution.

If staff break the rules as laid down by this policy they will lose temporary or permanent use of the school systems and will be subject to disciplinary proceedings. If the law has been broken the police will be informed and the school will assist the police with any prosecution.

Pupils with Additional Learning Needs

The school strives to provide access to a broad and balanced curriculum for all learners and recognises the importance of tailoring activities to suit the educational needs of each pupil. Where a pupil has specific learning requirements, or poor social understanding, careful consideration is given to the planning and delivery of e-safety awareness sessions and internet access.

Video-Conferencing and Webcams

The use of webcams to video-conference will be via our Internet Service Provider and therefore, subject which is our filtered service. Publicly accessible webcams are not used in our school setting.

Taking images via a webcam should follow the same procedures as taking images with a digital or video camera.

Permission should be sought from parents and carers if their child is engaged in video conferencing with individuals or groups outside of the school. This process should always supervised by a member of staff and a record of dates, times and participants held by the school.

Children need to tell an adult immediately of any inappropriate use by another child or adult. (This is part of the Acceptable Use Agreement).

Where children, young people (or adults) may be using a webcam in a family area at home, they should have open communications with parents/carers about their use and adhere to the Acceptable Use Agreement.

Managing Allegations against Adults Who Work With Children and Young People

In order to deal with any incidents that occur as a result of using personal mobile or e-mail technologies we refer to the Hampshire LA Guidance. The procedures detail how to deal with allegation of misuse or misconduct being made by any member of staff or child about a member of staff.

Allegations made against a member of staff should be reported to the Designated Safeguarding Lead (DSL) within the school immediately. In the event of an allegation being made against a Headteacher, the Chair of Governors should be notified immediately.

Local Authority Designated Officer (LADO) - Managing Allegations:

The Local Authority has Designated Officers who are involved in the management and oversight of individual cases where there are allegations against an adult in a position of trust. They provide advice and guidance to all of the above agencies and services, and monitor the progress of the case to ensure all matters are dealt with as quickly as possible, consistent with a thorough and fair process. In addition to this they liaise with the police and other agencies.

Disciplinary Procedure for All School Based Staff

In the event that a member of staff may be seen to be in breach of behaviour and good conduct through misuse of online technologies, this policy outlines the correct procedures for ensuring staff achieve satisfactory standards of behaviour and comply with the rules of the Governing Body.

Additional Information

Please be aware, at such time that you leave Bentley CE Primary School, your user account and any associated files, your email address and any associated emails will be removed from the school system and will no longer be accessible. The school cannot continue to receive emails sent to your email address.

If Pupils want a copy of any files within their user area, they may, during the last month of Year 6 at Bentley CE Primary School, seek support from the Computing Leader or a Technician who can copy their files to disk or memory stick.

If pupils, staff or parents do not understand any part of this Acceptable Use Policy, please ask the Headteacher for further guidance.

A copy of this policy can be accessed by visitors to the school's website

Personnel

The person responsible for E-Safety and Acceptable ICT Use is Zoe Hastie (Computing Leader).

We have a governor responsible for ICT who works closely alongside Zoe Hastie.