



Great Berry Primary School

Safe Internet Use Policy

Staff consulted:

Ratified by the Governing Body: Autumn 2026

Review Date: Autumn 2028

Use of the Internet (by pupils and staff) policy

Introduction

Often the resources used by pupils in school are carefully chosen by the class teacher and determined by curriculum policies. Use of the Internet, by its nature, will provide access to information which has not been selected by the teacher. Whilst pupils will often be directed to sites which provide reviewed and evaluated information, at time they will be able to move beyond these to sites unfamiliar to the teacher.

The problems and issues that have been highlighted by the media concerns all schools. Whilst some of the media interest is hype, there is genuine cause for concern that children might access unsuitable material either accidentally or deliberately.

The purpose of this policy is to:

- Establish the ground rules we have in school for using the Internet.
- Describe how these fit into the wider context of our discipline and PSHE policies.
- Demonstrate the methods used to protect children from sites containing pornography, racist or politically extreme views and violence. The school believes that the benefits to pupils from access to the resources of the Internet far exceed the disadvantages. Ultimately, the responsibility for setting and conveying the standards that children are expected to follow, when using media and information resources, is one the school shares with parents and carers.
- Offer guidance to staff about the use of social networking sites.

At Great Berry, we feel that the best recipe for success lies in a combination of site-filtering, of supervision, and by fostering a responsible attitude in our pupils in partnership with parents.

Using the Internet to enhance education

The benefits include:

- Access to a wide variety of educational resources including libraries, art galleries and museums;
- Rapid and cost-effective world-wide communication;
- Gaining an understanding of people and cultures around the globe;
- Staff professional development through access to new curriculum materials, expert knowledge and practice;
- Exchange of curriculum and administrative data with the Local Authority.
- Social and leisure use;
- Greatly increased skills in Literacy, particularly in being able to research, read and appraise critically and then communicate what is important to others;

- The schools intends to teach pupils about the vast information resources available on the Internet, using it as a planned part of many lessons;
- All staff will review and evaluate resources available on web sites appropriate to the age range and ability of the pupils being taught.

Pupils' Access to the Internet

Great Berry Primary School use RM SafetyNet filtered Internet service, which will minimize the chances of pupils encountering unsuitable material. Great Berry School will normally only allow children to use the Internet when there is a responsible adult present to supervise. However, it is unrealistic to suppose that the teacher's attention will always be directed towards every computer screen. Members of staff will be aware of the potential for misuse and will be responsible for explaining expectations of proper use to pupils.

Teachers will have access to pupils' emails and other Internet files generated in school, and will check these periodically to ensure that expectations of behaviour are being met.

Expectation of pupils using the Internet

- Pupils are expected to read and sign the 'E-Safety Class Agreement' at the beginning of every academic year. Once signed, the agreement is then displayed in all classrooms. **(appendix 1)**.
- Children in Early Years (EYFS) do not use the Internet or the Computers until Autumn 2 and so they will sign an adapted, simplified version of this document **(appendix 2)** later in the Autumn term. This is in accordance and in agreement with Dfe guidance and policy 'Teaching Online safety in school' updated in January 2023. We want to (as detailed in mentioned policy). To equip our pupils with the knowledge needed to make the best use of the internet and technology in a safe, considered and respectful way, so they are able to reap the benefits of the online world.
- At Great Berry we expect all pupils to be responsible for their own behaviour on the Internet, just as they are anywhere else in the school. This includes the materials they choose to access, and the language they use.
- Pupils using the World Wide Web are expected not to deliberately seek out offensive materials. Should any pupils encounter any such material accidentally, they are expected to report it immediately to a teacher, so that the website can be blocked by LH (Computing Co-ordinator), or DP (Headteacher) who can report this to RM to be blocked from school access immediately. The site can then be added as a 'web rule' to be filtered and therefore there will be no further access to the site.
- Every year at Great Berry, pupils and staff partake in 'Safer Internet Day'. During the Computing and PSHE lessons during that week, staff are expected to deliver lessons which enhance and teach the importance of how to stay safe online. The Computing lead should give appropriate lesson ideas and resources to class teachers to ensure the underpinning knowledge and behaviours which include *'how to evaluate what they (pupils) see online', how to recognise techniques used for persuasion,*

online behaviour, how to identify online risks, how and when to seek support'. (DFE, Teaching online safety in school: Guidance supporting schools to teach their pupils how to stay safe online, within new and existing school subjects, June 2019 Updated January 23). In addition to this, the computing lead and headteacher should deliver an assembly on online safety to all Early Years, Key Stage 1 and Key Stage 2 pupils.

- The importance of online safety is embedded into all Computing lessons and should always be reiterated and focused on in PSHE lessons taught in all year groups. This should *'complement the computing curriculum, which covers the principles of online safety at all key stages, with progression in the content to reflect the different and escalating risks that pupils face. (DFE, Teaching online safety in school: Guidance supporting schools to teach their pupils how to stay safe online, within new and existing school subjects, June 2019 Updated January 23).*
- All pupils learn 2 units each half term linked to Online Safety in the Purple Mash Scheme of Work to ensure this is woven into the curriculum for Computing. Online safety should form a fundamental part of a school's child protection and safeguarding measures. These units will be explored at the end of each half term.
- Pupils are expected not to use any rude or offensive language in their email communications, and contact only people they know or those the teacher has approved. They will be taught the rules of etiquette for email and will be expected to follow them.
- Pupils must ask permission before accessing the Internet and have a clear idea of why they are using it.
- Pupils must not access other people's files unless they have permission to do so.
- Computers and school laptops should only be used for school work and homework unless permission has been given otherwise.
- No program files may be downloaded from the Internet to the computer, to prevent corruption of data and to avoid viruses.
- No programs on flash drive/memory sticks should be brought in from home for use in school. This is for both legal and security reasons.
- No personal information such as phone numbers and addresses should be given out and no arrangements should be made to meet someone via the Internet/email, unless this is part of an approved school project.
- If pupils take photos or film video footage of themselves or others (children and staff members) on school grounds this should **not** be shared on any form of social media sites including Facebook, TikTok, Instagram or any other video/photograph sharing platform as this may put themselves and others at risk.
- Consent from the people in the images/videos must be given before they are taken. If consent given, then images/videos should be deleted once finished with and never shared on social media.
- Pupils consistently choosing not to comply with these expectations will be warned, and may be denied access to Internet resources. They will also be subject to the general disciplinary procedures of the school.

Appendix 1 – Pupil E-Safety Class agreement for safe computer and internet use:



Great Berry E-Safety Class Agreement



- 1) We remember to not post any personal information online – like our address, email address or mobile number.
- 2) We don't post pictures or videos of ourselves online. We know that once a picture goes online other people that we don't know may be able see it.
- 3) We don't befriend people we don't know online.
- 4) We don't meet up with people we have met and seen online.
- 5) We remember that not everyone online is who they say they are.
- 6) We respect other people's views, even if we don't agree.
- 7) If we see something online that makes us feel uncomfortable, unsafe or worried: we know we should leave the website, turn off the computer and tell a trusted adult immediately.
- 8) We know that if we are ever worried about something we have seen online we can talk to our Parents, carers or teachers at any time.
- 9) We know that some games and apps have an age restriction for a reason and so we do not use those.
- 10) We understand that not all information we see and read online is true and that we should check with an adult if we want to be sure.
- 11) If we are not sure of whether a website or email is real we will always ask a Parent/Carer or Teacher.
- 12) We always use technology and the Internet safely, respectfully and responsibly.
- 13) We understand that there will be consequences if we break the agreement and make ourselves vulnerable.

Appendix 2 – EYFS Pupil E-Safety Class agreement for safe computer and internet use



Great Berry EYFS E-Safety Class Agreement



- 1) Only use a computer when an adult is nearby.
- 2) Tell an adult straight away if you see something that upsets you.
- 3) Never talk to anyone online without an adult with you.
- 4) Never send anyone your picture.
- 5) Never tell anyone personal information about yourself, like your address or school name.
- 6) We respect other people's views, even if we don't agree.
- 7) If we see something online that makes us feel uncomfortable, unsafe or worried: we know we should leave the website, turn off the computer and tell a trusted adult immediately.
- 8) We know that if we are ever worried about something we have seen online we can talk to our Parents, carers or teachers at any time.
- 9) We know that some games and apps have an age restriction for a reason and so we do not use those.
- 10) We understand that not all information we see and read online is true and that we should check with an adult if we want to be sure.
- 11) Never tell anyone your password.
- 12) We always use technology and the Internet safely, respectfully and responsibly.

Early Years Screen time use- July 2026

In line with DFE guidance, 'Screen time should be limited to 1 hour a day, less if possible' for children aged between 2-5 years.

'All digital content should be:

- checked to ensure it is suitable for early years children, prior to showing it to the children.
-  slow-paced, repetitive and predictable - you should therefore avoid fast-paced, over-stimulating content - this includes content which has a lot of cuts, movement and flashing on screen, complex audio with lots of fast-talking characters or overlapping music and dialogue, or complex plots.
- advert-free, as young children cannot discern between advertisements and other content.
- free of scrolling and autoplay features, to ensure children are not inadvertently exposed to inappropriate content or able to access content for longer than planned use - this includes algorithm-driven content, such as video platforms.

All digital content should be:

- checked to ensure it is suitable for early years children, prior to showing it to the children.
- slow-paced, repetitive and predictable - you should therefore avoid fast-paced, over-stimulating content - this includes content which has a lot of cuts, movement and flashing on screen, complex audio with lots of fast-talking characters or overlapping music and dialogue, or complex plots.
- advert-free, as young children cannot discern between advertisements and other content.
- free of scrolling and autoplay features, to ensure children are not inadvertently exposed to inappropriate content or able to access content for longer than planned use - this includes algorithm-driven content, such as video platforms.

To follow these guidelines, we will ensure screen time is only used for use of short inputs for lessons.

Management of publishing on web platforms

Many schools have created websites that inspire children to publish work to a high standard, for a very wide audience. A website can celebrate children's work, promote the school and publish resources for projects or homework. Ground rules are important to ensure that the website reflects the school's ethos and that information is accurate and well presented.

As Great Berry Primary School's website can be accessed by anyone on the Internet, the security of staff and children is paramount. Although common in newspaper reports, the publishing of children's names beside photographs that identify individuals will not occur.

Editorial responsibility will lie with the Headteacher, even where parental help has been established to maintain the site. This is in order to ensure that content is accurate and the quality of presentation is monitored.

Staff and children will be made aware that the quality of their work published on the web needs to reflect the standard of work expected at Great Berry Primary School.

- The point of contact on the website should be the school address and telephone number. Home information or individual email identities will not be published.
- Full names will not be used anywhere on the website, particularly alongside photographs.
- Written permission from parents will be sought to give permission for the school to use photographs of their children on the website.

Appendix 3 - Employee ICT Acceptable Use Policy:

Introduction

ICT (including data) and the related technologies such as computers, email, the internet and mobile devices are an expected part of daily working life in school and the use of electronic communication and resources is encouraged.

All members of the school community are expected to use ICT responsibly and to comply with all applicable laws, policies and procedures, and with normal standards of professional and personal courtesy and conduct.

This policy is designed to ensure that all workers are aware of their professional responsibilities when using any form of ICT.

Failure to follow this policy may result in the withdrawal of access to school computers, email and internet and/or to disciplinary action, depending on the circumstances of the case.

Technology and the law change regularly and this policy will be updated as and when necessary. Workers will be informed when the policy has changed but it is their responsibility to read the latest version of this document.

1. Use of School Equipment/Networks

Computers, Mobile Phones and other devices provided by the school are loaned to individuals to support their professional responsibilities and must be used in accordance with this policy.

Workers are responsible for the safe and proper use, care and security of equipment and systems provided. Devices must be secured appropriately especially when leaving the school premises (i.e. not left unattended) and protected from unauthorised access or use (i.e. not accessed by family members). Any loss, damage or unauthorised access must be reported immediately.

Workers must not use school equipment, networks or system to access, download, send or receive, store, create, copy or distribute any material which may be malicious, illegal, libellous, immoral, dangerous or offensive (this includes but is not limited to pornographic, sexual, violent or criminal content and racist, sexist, or otherwise discriminatory material).

Any appropriate and authorised electronic communication with pupils or former pupils must be through official school network, channels, systems and on school equipment.

2.1 Remote/virtual learning

The same standards of conduct and behaviour and proper application of all policies and procedures are expected in virtual interactions with pupils as are required in person. In addition to following the other provisions within this policy and all other school policies:

- virtual connections should only be made where agreed and approved
- an adult should be present with the pupil where engagement is one to one
- dress codes should be observed
- virtual interactions should be in a neutral space - avoid personal spaces such as bedrooms and be aware of what is in the background on the screen

2. Use of Email

School business must always be conducted through official email addresses, which must be secured with password controls. Workers should respond to emails during working hours in a timely and appropriate fashion.

Email should be treated like any other form of written communication and, as such, the content should be appropriate and accurate and data protection compliant.

Extreme care must be taken with attachments from third parties, particularly unidentified third parties, as these may contain viruses.

Email must not be used to receive, send or forward messages that are defamatory, obscene or otherwise inappropriate. If such an email is received, whether unwittingly or otherwise and from whatever source, this must not be forwarded to any other address and must be reported immediately.

Reasonable access and use of the internet/intranet and email facilities is available to recognised representatives of professional associations' i.e. union officers for the performance of their official duties and activities.

3. Social Networks

Social networking applications include but are not limited to:

- Blogs
- Online discussion forums, for example Facebook;
- Media sharing services for example YouTube;
- Professional networking sites, for example Linked In
- 'Micro-blogging' application for example Twitter

Where the school operates official networking sites, these must be managed and used in accordance with this policy. This includes the following requirements:

- use of official (i.e. not personal) email addresses for user accounts;
- appropriate feedback and complaints information must be published in a prominent place which is easily accessible to other users;
- the school's logo and other branding elements should be used to indicate the school's support. The school's logo should not be used on social networking applications which are unrelated to or are not representative of the school's official position;
- users should identify themselves as their official position held within the school on social networking applications e.g. through providing additional information on user profiles;
- any contributions on any social networking application must be professional, uphold the reputation of the school and be in accordance with data protection requirements;
- users must not promote or comment on personal matters (including personal/ financial matters), commercial ventures, political matters or campaigns, religion or other matters;

4. Personal use of school Equipment/Networks

School equipment, internet services, systems and email may be used for incidental personal purposes, with the approval of the line manager, provided that it:

- does not interfere with the school's operation of computing facilities or email services; does not interfere with the user's employment or performance of professional duties or other obligations to the school;
- is of a reasonable duration and frequency;
- is carried out in authorised break times or outside their normal working hours;
- does not over burden the system or create any additional expense to the school;
- is not used to access, send, receive or store inappropriate material; and
- does not bring the school and its community into disrepute.
- Workers must notify the school of any significant personal use.

Reasonable access and use of the internet/intranet and email facilities is available to recognised representatives of professional associations' i.e. union officers for the performance of their official duties and activities.

Email should be treated like any other form of written communication and, as such, the content should be appropriate and accurate and data protection compliant.

School equipment/networks/systems must additionally not be used for

- commercial purposes not under the auspices of the school;
- personal financial gain;
- personal use that is inconsistent of other school policies or guidelines; or
- ordering of goods to be delivered to the school address or in the school's name.

5. Use of personal ICT equipment in school

6.1 Mobile Phones

It is accepted that individuals may bring personal mobile phones to school. Personal mobiles should have security codes to prevent access by other persons and must be stored securely and not accessible to pupils at any time.

Workers are not permitted to use their personal mobile phones to call, text, email or in any other way message pupils. Nor may they divulge their personal telephone number(s) or other contact details to pupils under any circumstances.

Workers are required to ensure mobile telephones are switched off/to silent during working hours and accessed only during authorised breaks. Phones should not be used in front of pupils, except in an emergency where workers can use their phones to contact the school office or a senior member of staff. Any urgent phone calls or messages must be directed to the office who will notify workers immediately. Workers who need to use their mobile telephone to make or receive an urgent call during working hours should where possible obtain prior authorisation from their line manager to do so.

5.2 Other electronic devices

Workers should not bring other electronic devices onto school premises unless this has been specifically authorised by an appropriate manager. In such circumstances, the computer / equipment must be kept securely (at the risk of the owner) and security protected so that it cannot be accessed by pupils or others at the school.

Any personal use of such equipment must be restricted to an employee's break times or outside their normal working hours and must not impact on their duties in any way.

Additionally, specific permission must be obtained prior to connecting any device to school networks/systems and the device(s) must have adequate virus protection.

Workers must ensure that no personal information regarding school business, its pupils or staff is stored on such personal equipment.

Where exceptionally, specific permission is granted to use personal equipment for work purposes e.g. to give a presentation, the employee must be extremely vigilant that personal files/data etc. are not inadvertently accessed or displayed.

Pictures or videos that are taken within school or at any school related activity, should not be taken on personal devices. Pictures or videos must only be taken on school devices.

6. Personal social networks

The school recognises individual rights to privacy and a private life. However, the law generally views social media as in the public domain, irrespective of privacy settings. Workers are therefore advised to be mindful of their duties and obligations to uphold the reputation of the school, to comply with the Code of Conduct and other policies and contractual terms in their use of personal social media - being mindful of the real possibility for material to be posted, shared and made public inadvertently or by other contacts.

The school may require the removal of content it considers inappropriate.

It is totally unacceptable for any worker to discuss pupils, parents, work colleagues or any other member of the school community or any school related business on any type of social networking site.

Other posting on personal sites may also impact on the reputation of the school or the suitability/conduct of the employee for example if an employee is off sick but makes comments on a site to the contrary, postings of indecent or inappropriate images/activities etc.

Workers must not accept or propose contact, nor engage in any conversation with pupils on any personal social networking sites. Workers should also avoid personal network contact with former pupils, particularly those under the age of 18 years. - any relevant contact with ex-pupils should be through school channels and agreed with school leaders. Individuals working in the school should not use or access social networking sites of pupils.

7. Security

The school follows sound professional practices to secure data, system programmes, email records and networks under its control.

Workers must take all reasonable precautions to maintain security and confidentiality and to protect data. This includes:

- using appropriate security measures such as encryption/password protection to transmit confidential or sensitive information;
- ensuring all devices and system access are password protected Using secured memory sticks (all laptops, memory sticks and devices used must be encrypted);
- ensuring that pupils are not exposed to any inappropriate images or web links; and
- respecting all copyrights and not copy, retrieve, modify or forward copyrighted materials except as permitted by the copyright owner.

Users must not:

- use, transfer or tamper with other people's accounts and files;
- use anonymous mailing services to conceal identity when mailing through the Internet, falsify e-mails to make them appear to originate from someone else, or provide false information to any Internet service which requests name, e-mail address or other details;
- use electronic media and services in a manner that is likely to cause network congestion or significantly hamper the ability of other people to access and use the system;
- permanently store sensitive or confidential data on their own equipment - this extends to personal cameras, mobile phones and other similar devices;
- use the internet/intranet facilities or equipment to deliberately create any virus, worm, Trojan horse or any such other programme that is harmful to normal computer operations.
- monitor or intercept the files or electronic communications of other workers or third parties;
- hack or obtain access to systems or accounts they are not authorised to use;
- use other people's log-ins or passwords; or
- breach, test, or monitor computer or network security measures without authorisation.

Where any security breach or inappropriate connection or ICT activity occurs, the user must immediately disconnect/log out and report immediately.

8. Privacy and Monitoring

The school respects workers' privacy and will not routinely inspect or monitor emails, data or internet usage.

However, workers should not have any expectation of absolute privacy in his or her use of the school systems or equipment (including but not limited to

networks/servers/internet usage/networks/Wi-Fi). Under the following circumstances the school reserves the right, at its discretion, to review any electronic files and messages to the extent necessary to ensure systems are being used appropriately:

- when required by law;
- if there is a substantiated reason to believe that a breach of the law; or school's policy has taken place;
- if the school suspects that the employee has been viewing/transmitting offensive or illegal material;
- if the school suspects that the employee has been spending an excessive amount of time on activity which is not work related;
- where required for compliance checks e.g. auditors, data protection; or
- where there are emergency or compelling circumstances.

The school will endeavour to notify affected individuals of any monitoring which will take place and the reason for it, save in exceptional circumstances (see below).

Workers will normally be notified of what information will be recorded and retained, and for how long, who will have access and how such information will be used, which will include using such information for disciplinary purposes where applicable.

When monitoring emails, the school will, save in exceptional circumstances; confine itself to looking at the address and heading of the emails. Workers should mark any personal emails (where these are permitted by the school) as such and encourage those who send them to do the same. The school will avoid, where possible, opening emails clearly marked as private or personal.

The school considers the following to be valid reasons for checking an employee's email:

- if the employee is absent for any reason and communications must be checked for the smooth running of the school to continue;
- if the school suspects that the employee has been viewing or sending offensive or illegal material, such as material containing racist terminology or nudity (although the school understands that it is possible for workers inadvertently to receive such material and they will have the opportunity to explain if this is the case);
- if the school suspects that an employee has been using the email system to send and receive an excessive number of personal communications (or any personal emails if this is prohibited by the school); and
- if the school suspects that the employee is sending or receiving emails that are detrimental to the school or its pupils.

The school may monitor communications without notification in certain specific circumstances, including but not limited to;

- establish the existence of facts relevant to the school e.g. whether a contract was entered into by email;
- ascertain compliance with regulatory or self-regulatory practices e.g. checking that the school is complying with external or internal regulations;

- ascertain or demonstrate standards that are or ought to be achieved by workers using the system;
- investigate or detect unauthorised use of the telecommunication system, which would include checking that workers are not breaching the school's policy on email and internet use; and
- ensure the effective operation of the system, for example through virus monitoring.

Monitoring will be reasonable and in accordance with current legislation.

9.1 Covert monitoring

The use of covert monitoring will only be used in exceptional circumstances, for example, where the school suspects criminal activity or where telling the employee about the monitoring would make it difficult to prevent or detect such wrongdoing.

If the school considers covert monitoring to be justified, this will only take place as part of a specific investigation and will cease when the investigation has been completed.

Acceptable Use Agreement

Introduction

Our school promotes the positive use of technology and assists in developing pupil's knowledge and understanding of digital devices and the internet. We have a duty of care to safeguard pupils when using technology in our academies. This agreement is designed to ensure that all staff, governors, volunteers, visitors and contractors understand their professional responsibilities when using any form of ICT in our academies.

Agreement

I understand my role and responsibility in using ICT (including data) and related technologies such as email, the internet and mobile devices at Great Berry as detailed below:

1. I will only use the Trust's email/internet/intranet/learning platform and other related technologies for professional purposes or for uses deemed reasonable by the Headteacher or Governing Body.
2. I am aware that all network and internet activity is logged and monitored and can be made available, on request, to the Headteacher in the event of allegations of misconduct.
3. I will not write or upload any defamatory, objectionable, copyright infringing or private material, including images and videos of pupils, parents or staff on social media or websites in any way which might bring the school into disrepute.
4. I will not browse, download or upload or distribute any material that could be considered offensive, illegal discriminatory or copyright infringing.
5. I will only use authorised browser apps. i.e Purple Mash, SchoolsBuddy to post information to parents and pupils.
6. I will only use the approved, secure email system(s) for any academy business.
7. Photographs of staff, pupils and any other members of the school community will not be used outside of the internal school IT network unless written consent has been granted by the subject of the photograph or their parent/guardian.
8. I will not install software onto the Trust network unless I have received express permission from the Headteacher.
9. I will ensure that personal data is kept secure and is used appropriately, whether on academy premises, taken off academy premises or accessed remotely. Personal or sensitive data taken off site must be encrypted and will not be stored on any personal IT equipment.
10. I will not divulge any Trust related passwords and I will comply with Trust IT security procedures.
11. I will ensure that my mobile phone and any other personally owned device is switched off or switched to 'silent' mode when I have directed time with pupils. I will only make or receive calls in specific designated areas such as the staff room and only use personal devices for work purposes when in front of pupils during the school day.
12. I will not give out my own personal details, such as mobile phone number, personal e-mail address and social networking identities to parents or pupils.
13. I will report any incidents of concern regarding pupil's safety to the academy's E-Safety Co-ordinator or the Designated Child Protection Officer. Our ISP, RM has monitoring and alerting in place and will notify the headteacher accordingly.
14. I will support and promote the Trust's E-Safety and Data Security policies and help pupils be safe and responsible in their use of ICT and related technologies.
15. I will abide by the school ICT acceptable use policy which can be found in the current code of conduct

Signature: _____ Date: _____

Print Name: _____

Role in School: _____

Signature of School Representative: _____ Date: _____