



Online Safety (E-safety) Policy

Contents

1. Introduction
2. Context- The internet and online technologies
3. Roles & Responsibilities
4. Portable Storage media
5. Online Safety Curriculum
 - a) Internet access at school
 - b) Using the internet for learning
 - c) Teaching the safe use of the Internet
 - d) Using email
 - e) Chat and online discussions
 - f) Other online technologies – mobile phones etc
 - g) Cyberbullying
 - h) Peer on Peer Abuse
 - i) Radicalisation & Extremism
 - j) Creating and sharing images/videos
 - k) Deliberate misuse-Procedures and Sanctions
 - l) Remote Learning
6. Complaints
7. Policy Decisions authorising Internet access
- Appendix:
 - I. Pupil Acceptable Use Agreements (EYFS/KS1/KS2)
 - II. Staff Acceptable Use agreement form
 - III. Smart Rules Poster
 - IV. Remote learning Acceptable Use
 - V. Links to School Documents
 - VI. Links to Government Documents

Revised by: Helen Phillips (Computing subject Lead)

Last Revised : December 2023

To be revised : annually



1. Introduction

Our Online Safety Policy has been written with reference to national example policies and Government guidelines and links with other related school policies (see Appendix vi/vii) It has been read by and discussed with staff, agreed with senior management and approved by Governors.

It will be reviewed annually

It is the duty of the school to ensure that every child in our care is safe and the principles that would be applied in a physical school setting can be applied in the 'digital' or 'virtual' world. We want to ensure our pupils create a positive digital footprint.

The policy has been drawn up to protect all parties: the pupils, staff and the school and aims to provide clear advice and guidance on how to minimise risks and how to deal with any infringements.

2. Context – the internet and online technologies

New internet and online technologies are enhancing communication and the sharing of information. They are an essential element in 21st century life for education, business and social interaction. Current internet and online technologies, some used in school, but more importantly used by many pupils outside include:

- The internet – World Wide Web
 - Smart phones with unlimited and unsupervised access
 - Games consoles (e.g. X-box/PS4) with online access
- Email
- Web-based video calls (e.g Skype)
- Online chat rooms and discussion forums
- Social media sites (e.g. Facebook, Instagram)
- Music and video downloading (itunes, spotify)
- Video broadcasting apps (Tiktok/youtube)
- Mobile phones with camera and video functionality

At Berridge, we aim to educate and encourage pupils to use technology appropriately and safely by creating a safe ICT learning environment through:

- Policies and procedures, with clear roles and responsibilities
- Embedding online safety within the school curriculum and schemes of work.
- Using a range of devices, software and apps.



3. Roles and Responsibilities

We recognise the importance of online safety in today's world and have a whole school approach to embedding online safety practices.

Senior Leadership team- SLT ensure that the policy is implemented across the school through the monitoring process. Investigate any online-safety alerts identified by our managed monitoring system.(see section 7)

DSL / Technical Lead- is responsible for keeping up to date on all online safety issues and ensuring that staff are updated as necessary and ensuring that there is a robust online safety scheme of work.

Governors- The Governing Body is responsible for overseeing and reviewing all school policies including the Online safety policy.

School staff - All teaching staff are responsible for promoting and supporting safe online behaviours and following school online safety procedures ensuring that they:

- Have read and understood the parts relating to online safety in the **KCSIE**
- have read, understood and signed the Staff Acceptable Use Policy (AUP) (Appendix ii)
- have an up to date awareness of online safety matters and of the current school Online Safety Policy and procedures.
- Report any suspected misuse or problem to the DSL (Designated Safeguarding Lead) and the Online Safety Lead for investigation, action or sanction and log on C-POMS
- Digital communications with pupils should be on a professional level and only carried out using official school systems.
- Online safety issues are embedded in all aspects of the curriculum and other school activities
- Ensure pupils understand and follow the school online safety rules and Pupil acceptable use policy
- Monitor pupil's online activity in lessons and extra-curricular school activities
- In lessons where internet use is pre-planned pupils should be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches.
- Address issues that may arise from pupils' research regarding biased views. Link to 'R' of SMART ❤️ rules, which is reliable.
- Class teachers should ensure that pupils are aware of the SMART ❤️ rules (Appendix iii), introducing them at the beginning of each new school year; then embedding them with regular discussions.

Pupils- pupils are expected to take an active part in the planned lessons and activities to support their understanding and confidence in dealing with online safety issues, both at home and at school. They are asked to:

- Follow the school online safety rules
- Understand and follow the guidance set out in the pupil acceptable use policy (Appendix i)
- Be a responsible user of digital technology
- Talk to a trusted adult if they have any questions or concerns relating to online activity

Parents – parents and carers play a crucial role in ensuring that their children understand the need to use the internet and mobile devices in an appropriate way. They will be responsible for endorsing the Pupil Acceptable use Policy. We support the Parents' and Carers' in this role by:



- Drawing parents and carers attention to the School Online Safety Policy in newsletters and on the school website.
- Providing parents and carers with advice on online safety issues
- Maintaining a list of online safety resources for parents' and carers' to access.

Technical Support – The school's technical support is provided by Schools IT. Our managed service technician visits the school on Thursdays to maintain our hardware, software and computing infrastructure.

Our technician aims to keep our system safe and secure by:

- Reviewing the school computing infrastructure and ensuring it remains secure and not open to misuse or malicious attack.
- Updating all security software regularly
- Discussing security strategies annually with the Technical Lead and Senior Leadership Team.
- Working in partnership with IT services and Net Sweeper to ensure filtering systems to protect pupils are reviewed and improved.
- Regularly checking that the filtering methods selected are appropriate, effective and reasonable.
- Ensuring users may only access the school's network through a properly enforced password.

4. Portable Storage media – staff are allowed to use their own portable media storage (USB sticks etc) but no sensitive data should be taken from the premises. Sensitive data must be stored on the secure school network and if it has to be taken from the premises it should be saved on a password protected (BITLOCKER) portable storage device, in line with the school's GDPR Policy (Appendix v) and the **Data Protection Act (2018)** (Appendix vi)

5. Online Safety Curriculum

a) Internet Access –

- Use of Internet by pupils** - internet access is carefully controlled by teachers according to the age & experience of the pupils, and learning objectives being addressed. Pupils are always actively supervised by an adult when using internet.
 - Access for all** – in line with our inclusion policy, we want to ensure that all pupils have access to the internet, particularly where this will directly support their learning.
- b) Using the internet for learning-** the internet is now an invaluable resource for learning for all of our pupils, and we use it across the curriculum both for researching information and a source of digital learning.

Internet use is a statutory part of the **Computing Curriculum (2014)** (Appendix vi) pupils are taught how to find appropriate information on the internet and to ensure, as far as that is possible, have the skills to evaluate how accurate and truthful it is.

- Pupils are taught how to use search engines and how to evaluate internet-based information
- Pupils are taught how to recognise the difference between commercial and non-commercial web sites, and how to investigate possible authors of web-based materials

- They are taught how to carry out simple checks for bias and misinformation
- They are taught that web based resources have similar copyright status as printed and recorded materials, and that this must be taken into consideration when using them.

c) **Teaching safe use of the internet & online technologies**— it is crucial to teach pupils how to use the internet and other online technologies safely, both at school and at home.

Teaching pupils how to be safe, respectful and responsible users of technology is a statutory part of the **Computing curriculum (2014)** Recognising how online technologies can impact on physical and mental wellbeing is now a statutory part of **Health Education (2020)**. Online relationships, is a statutory part of **Relationships Education (2020)**

We have developed an Online Safety program in line with the guidance set out in **‘teaching online safety in schools’ June 2019** and use resources from a number of places, including **Education for a connected World (2020)** and **Childnet**- The main aspects of this approach include following the five **SMART♥rules** when online.

(see appendix vi)

Suitable material – We encourage pupils to see the internet as a rich and informative resource but it can be difficult to navigate and find appropriate material. Where possible, particularly with the younger pupils, we provide pupils with suggestions for suitable sites, and staff always check the suitability of websites before suggesting them to pupils or using them in their teaching.

Non-Education materials – as well as curriculum related material, we encourage pupils to visit appropriate entertainment and child-oriented activity sites that have interesting and relevant activities, games and information, at home.

Unsuitable material- Occasionally pupils, despite all the security provision in place, may come across something on the internet that they find offensive, unpleasant or distressing. Pupils are taught to always report such experiences directly to an adult at the time they occur, so that action can be taken.

The action will include:

1. Making a note of the website and any other websites linked to it
2. Informing the Technical Lead, who will report the incident to the technician if a site needs blocking
3. Logging the incident – Online Safety Incident Log Book
4. Discussion with the pupil about the incident, and how to avoid similar incidents in future.
5. Informing parent or carer
6. Log on C-POMS, if concerned that pupils’ may have knowingly searched for inappropriate material

d) E-mail – Email is a valuable method of communication. Pupils need to understand the role of e-mail, and how to use it appropriately and effectively. We teach the use of E-mail as part of the computing curriculum and use appropriate pupil email accounts as it is an important communication skill. Pupils only use their email accounts in school where we can monitor and regulate their accounts to ensure they are being used appropriately and safely.

Pupils are not allowed to use personal emails at school or use their school email for anything other than teacher directed activities.

Some online software that we use as part of the curriculum is now based online e.g. Teams, Scratch, Google Sketchup, the pupils use their emails to create accounts so that they can access the resources.

Students will be taught to:

- immediately tell a teacher if they receive something upsetting.
- not reveal their personal details or those of others, or arrange to meet anyone without specific permission
- treat incoming e-mail as suspicious and that attachments should not be opened unless the sender is known

e) Chat, discussion and social networking sites- pupils do not currently access these forms of electronic communication but they are being used by more and more pupils outside of school. Online chat rooms, discussion forms and social networking sites present a range of personal safety and privacy issues. With this in mind pupils will be given guidance on how to use these forms of communication safely and responsibly. This will include:

- never to give out personal details of any kind which may identify them, their friends or their location.
- not placing personal photos on any social network space without considering how the photo could be used now or in the future.
- only inviting known friends and denying access to others when using social networking and instant messaging services.
- being advised on privacy settings and encouraged to set passwords, to deny access to unknown individuals and to block unwanted communications.

f) Internet enabled mobile phones and handheld devices- More and more young people have access to internet-enabled devices such as SMART phones. Pupils will be taught:

- the legal and moral implications of posting photos and personal information from their phones to public websites
- how the data protection and privacy laws apply
- about consent to having their photo taken; emphasising the need to be 'share aware' (NSPCC)

- about the growing threat of 'sexting' (Y5/6) emphasising the implications of taking indecent images of themselves, or allowing other to do so, if they are shared around or become viral
- g) Cyberbullying- Online bullying or harassment** – Online bullying or harassment via instant messaging, texting, email, and chat rooms are potential problems that can seriously impact of pupils mental wellbeing.
- Our school has a range of strategies and policies to prevent online bullying. These include:
- No access to public-chat rooms, instant messaging, bulletin boards or social media sites when at school.
 - Complaints of cyberbullying are dealt with in accordance with our Behaviour Policy (appendix vi)
 - Complaints relating to child protection are dealt with in accordance with procedures detailed in our Safeguarding policy (appendix v)
 - Cyberbullying is regularly addressed through the Online safety program we have devised.
 - Pupils are encouraged to discuss their concerns or worries about online bullying or harassment with staff or a trusted adult
 - This is consolidated with **Tell** rule- (the 't' in the SMART rules) which reiterates the need for pupils to tell someone about any concerns or fears they may have.
- h) Child on Child Abuse** – We strongly recognise the risk of child on child abuse taking place online-both in and outside of school.
- All staff should be clear as to the school's safeguarding policy and procedures with regards to child on child abuse and the important role they have to play in preventing it and responding where they believe a child may be at risk from it. (See safeguarding Policy appendix v and KCSIE appendix vi)
- All members of staff should recognise the range of online peer one peer abuse safeguarding issues and understand how they should respond to and report concerns.
- Online child on child abuse is most likely to include, but may not be limited to:*
- **bullying** -including cyberbullying, prejudice-based and discriminatory bullying
 - **physical abuse** -this may include an online element which facilitates, threatens and/or encourages physical abuse
 - **sexual violence** - this may include an online element which facilitates, threatens and/or encourages sexual violence
 - **sexual harassment**- such as online sexual harassment,which may be standalone or part of a broader pattern of abuse
 - **Sexting**- consensual and non-consensual sharing of nudes and semi-nude images and or videos
 - **upskirting**, which typically involves taking a picture under a person's clothing without their permission, with the intention of viewing their genitals or buttocks to obtain sexual gratification, or cause the victim humiliation, distress or alarm
 - **initiation/hazing type violence and rituals** - may include an online element
- i) Radicalisation and Extremism**- We strongly recognise the risk of on-line radicalisation through the use of the internet and social media. To combat this, we use Local Authority approved filtering system, which block sites with inappropriate content, including extremist content.



Berridge Primary School Online Safety Policy

If a member of staff comes across any articles, videos, speeches, images online that promote terrorism or promote violence or hatred towards others they must report it to a DSL or member of SLT.

This is in accordance with procedures outlined in the PREVENT section of the Safeguarding policy. (appendix v)

- j) Creating of / sharing of images & videos-** from time to time activities may involve recording images or videos for their curriculum work, displays, to celebrate achievements, for publicity etc.

However, images/videos are not recorded without written permission from a parent or guardian. Without permission children's images will not be used. Parents/carers sign a photograph consent form, held in the school office, when their child first starts at the school.

Images and videos are considered to be personal data and as such are treated in accordance with guide lines set out in the GDPR policy (Appendix v) and the **Data Protection Act 2018** (Appendix vi)

- k) Deliberate misuse of internet facilities** – Rules for Internet Safety and appropriate use are discussed and displayed in classrooms.

Where a pupil is found using the internet inappropriately, for example to download games, search for some unsuitable images, then sanctions will be applied according to the nature of the misuse, and any previous misuse.

Sanctions will include:

- Initial warning from the class teacher
- Letter to parent /carer

For Offensive material (e.g racist, sexist, or other hate websites/images)

- Incident logged and reported to the headteacher
- Initial letter to parent /carer
- Removal of internet privileges

- l) Remote Learning-** please see the Acceptable Use Policy for Remote Lessons (appendix iv)

- m) Mobile phones-** Mobile phones are not allowed in schools for pupils in Year 4 or below. Pupils in Y5/6 may be granted permission to bring phone to school in exceptional circumstances. Please see Mobile Phone Policy (appendix v)

6) Complaints - Handling online safety complaints:

- Complaints of internet misuse will be referred to the online safety coordinator.
- Any complaint about staff misuse will be referred to the Head Teacher.
- Complaints of a child protection nature must be dealt with in accordance with the school child protection procedures and referred to the DSL (Designated Safeguarding Lead)

Staff and pupils are given information about the acceptable use of digital technologies and are aware that infringements may result in a sanction.

Possible sanctions, depending on the severity of the infringement:



Berridge Primary School Online Safety Policy

- Incident will be recorded
- Interview/counselling by class teacher, online safety lead, SLT, headteacher, DSL, (dependent on incident)
- Informing parents
- Removal of internet/ computing access for a period
- Referral to LA/Police

7. Filtering & Monitoring Standards – The Department for Education’s statutory guidance [‘Keeping Children Safe in Education’](#) obliges schools and colleges in England to “ensure appropriate filters and appropriate monitoring systems are in place and regularly review their effectiveness” and they “should be doing all that they reasonably can to limit children’s exposure to the above risks from the school’s or college’s IT system” however, schools will need to “be careful that “over blocking” does not lead to unreasonable restrictions as to what children can be taught with regards to online teaching and safeguarding.”

School works closely with Schools IT to ensure that the school’s digital infrastructure is compliant with all legal safety requirements, including the KCSIE. (See *roles & Responsibilities section 3*)

School uses Smoothwall Monitoring which is a digital monitoring solution that flags incidents as they happen by real-time monitoring of both keystroke and screen view activity by users. DSLs in the leadership team are alerted when users try to type or view harmful or inappropriate material.

8. Policy Decisions authorising Internet access- The school takes reasonable precautions to prevent access to inappropriate material. However, due to the international scale and linked nature of internet content, it is not possible to guarantee that unsuitable material will never appear on a computer connected to the school network.

The school cannot accept liability for any material accessed, or any consequences of internet access, although it will do all that is possible to reduce the risk of inappropriate material being accessed.

The Technical Lead and technician will monitor the network regularly to establish that the online safety policy is adequate and that the implementation of the online safety policy is appropriate and effective.

Appendix:

- I. Pupil Acceptable Use Agreements [Pupil AUPs](#)
- II. Staff Acceptable Use Agreement [Staff AUP](#)
- III. Smart Rules Poster [SMART Rules Poster](#)
- IV. Remote Learning Acceptable Use [remote learning AUP](#)
- V. Links to School Policies [school policies](#)
- VI. Links to Government Documents [Government Links](#)
- VII. Link to Data Protection Act <https://www.gov.uk/data-protection>