BRIDGEWATER PRIMARY SCHOOL

Online Safety and Acceptable Use Policy

Version: 1.1

Version No.	**Date**	**Author**	**Comments**
1.0	08-08-2023	Mrs Redden	Policy updated to reflect DfE filtering and monitoring standards and updates to KCSIE 2023
1.1	12-12-2023	Mrs Redden	Policy updated to comply with the new statutory Early Years Legislation.

Bridgewater Primary and Nursery School
Online Safety and Acceptable Use Policy

Reviewed September 2023. This policy is reviewed annually.
Online Safety Leader: Nicola Redden

Information and Communications Technology (ICT) is seen in the 21st Century as 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, schools need to build in the use of these technologies in order to arm our young people with the skills to access life-long learning and employment.

ICT 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 ICT within our society as a whole. Currently the internet technologies children and young people are using both inside and outside of the classroom include:

- Websites
- Virtual Learning Environments
- E-mail and Instant Messaging
- Chat Rooms and Social Networking
- Blogs and Wikis
- Podcasting
- Video Broadcasting
- Music Downloading
- Gaming
- AI technology
- Mobile/ Smart phones with text, video and/ or web functionality
- Other mobile devices with web functionality and wearable technology e.g smart watches

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.

Bridgewater Primary and Nursery School ensures that all children have access to the Computing curriculum and resources, regardless of ethnicity, gender, economic background, class or ability.

At Bridgewater Primary and Nursery School**,** we understand the responsibility to educate our pupils regarding Online Safety issues; teaching them the appropriate behaviours and critical thinking skills to enable them to remain both safe and legal when using the internet and related technologies, both in and beyond the context of the classroom.

Both this policy and the Acceptable Use Agreement (for all staff, governors, visitors, parents/carers and pupils) are inclusive of both fixed and mobile internet; technologies provided by the school (such as PCs, laptops, tablets, webcams, whiteboards, voting systems, digital video equipment, etc); and technologies owned by pupils, parents, staff and visitors but brought onto school premises (such as laptops, mobile phones, camera phones, smart watches/fitness trackers and portable media players, etc).

The aims of this policy are to:

- Set out the key principles expected of all members of the school community at Bridgewater Primary and Nursery School with respect to the use of IT-based technologies.
- Safeguard and protect the children and staff of Bridgewater Primary and Nursery School using the internet, social media or mobile devices
- Assist school staff working with children to work safely and responsibly with the internet and other communication technologies and to monitor their own professional standards and practice to role model positive behaviour online.
- 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 online bullying, 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.
- Ensure the curriculum teaches children how to make the correct choices online and know whom to speak to enable them to keep safe.
- Minimise the risk of misplaced or malicious allegations made against adults who work with children.
- The school will act in accordance with the Prevent Duty, which explains the schools' duties under the Counter-Terrorism and Security Act 2015 with respect to protecting people from the risk of radicalisation and extremism.
- Take into account the DfE statutory guidance 'Keeping Children Safe in Education' 2021 and Statutory Framework for Early Years and Foundation Stage 2021.

The main areas of risk for our school community can be summarised as follows:

Content

- exposure to inappropriate content, including online pornography, ignoring age ratings in games (exposure to violence associated with often racist language), substance abuse
- lifestyle websites, for example pro-anorexia/self-harm/suicide sites
- hate sites
- content validation: the need to check authenticity and accuracy of online content

Contact

- grooming and/or exploitation for sexual, criminal, financial or other purposes
- online bullying in all forms
- identity theft (including 'frape' (hacking Facebook profiles)) and sharing passwords

Conduct

- privacy issues, including disclosure of personal information
- digital footprint and online reputation

- health and well-being (amount of time spent online (Internet or gaming))
- sending and receiving of explicit images (consensual and non-consensual sharing of nude or semi-nude images and/or videos) also referred to youth produced sexual imagery
- up skirting
- initiation/hazing type violence and rituals
- extremism
- copyright (care or consideration for intellectual property and ownership – such as music and film).

Commerce

- risks such as online gambling
- inappropriate advertising
- phishing and or financial scams

(Ref Inspecting e safety Ofsted 2014, KCSiE 2023)

Scope

This policy applies to all members of Bridgewater Primary and Nursery School community, including staff, students, pupils, volunteers, parents, carers and visitors.

The Education and Inspections Act 2006 empowers Headteachers to such extent as is reasonable, to regulate the behaviour of pupils when they are off the Bridgewater Primary School site and empowers members of staff to impose disciplinary penalties for inappropriate behaviour (also see the Behaviour Policy). This is pertinent to incidents of cyber-bullying, or other online safety incidents covered by this policy, which may take place outside Bridgewater Primary and Nursery School but is linked to membership of the school. The 2011 Education Act increased these powers with regard to the searching for and of electronic devices and the deletion of data.

Bridgewater Primary and Nursery School will deal with such incidents within this policy and the Anti-bullying policy and will, where known, inform parents / carers of incidents of inappropriate online safety behaviour that takes place out of school.

Review and Monitoring

The importance of online safety is referenced within other school policies: Safeguarding policy, Behaviour policy, Anti-bullying policy, British Values Statement, and Personal, Social and Health Education policy.

- The school has an Online Safety Coordinator who will be responsible for document ownership, review and updates.
- The Online Safety policy will be reviewed annually or when any significant changes occur with regard to the technologies in use within the school.
- The Online Safety policy has been written by the school Designated Safeguarding Leader (DSL) alongside the Online Safety Coordinator 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 Governors. All amendments to the school online safeguarding policy will be discussed in detail with all members of teaching staff.

Authorised ICT staff (The DSL and The Online Safety Coordinator) may inspect any ICT equipment owned or leased by the school at any time without prior notice. If you are in doubt as to whether the individual requesting such access is authorised to do so, please ask for their identification badge and contact the Headteacher. Any ICT authorised staff member will be happy to comply with this request.

All monitoring, surveillance or investigative activities are conducted by ICT authorised staff and comply with the Data Protection Act 2018, the Human Rights Act 1998 and the Regulation of Investigatory Powers Act 2000 (RIPA), KCSiE 2023, DfE Filtering and Monitoring Standards 2023.

Please note that personal communications using school ICT may be unavoidably included in any business communications that are monitored, intercepted and/or recorded.

Breaches

A breach or suspected breach of policy by a school employee, contractor or pupil may result in the temporary or permanent withdrawal of School ICT hardware, software or services from the offending individual.

Any policy breach is grounds for disciplinary action in accordance with the School Disciplinary Procedure or, where appropriate, the local authority Disciplinary Procedure or Probationary Service Policy.

Policy breaches may also lead to criminal or civil proceedings.

Incident Reporting

Any security breaches or attempts, loss of equipment and any unauthorised use or suspected misuse of ICT must be immediately reported to the Headteacher or Online Safety Coordinator. Additionally, all security breaches, lost/stolen equipment or data (including remote access Secure ID tokens and PINs), virus notifications, unsolicited emails, misuse or unauthorised use of ICT and all other policy non-compliance must be reported to the Headteacher or Online Safety leader.

Computer Viruses

- All files downloaded from the Internet, received via e-mail or on removable media (e.g. USB Stick or CD) must be checked for any viruses using school provided anti-virus software before using them.
- Never interfere with any anti-virus software installed on school ICT equipment that you use.
- If your machine is not routinely connected to the school network, you must make

provision for regular virus updates through your IT team.

- If you suspect there may be a virus on any school ICT equipment, stop using the equipment and contact your ICT support provider immediately (EasiPC). The ICT support provider will advise what actions to take and be responsible for advising others that need to know.

Equal Opportunities for Pupils with Additional Needs

The school endeavours to create a consistent message with parents and carers of all pupils and this in turn should aid establishment and future development of the school's online safety rules.

However, staff are aware that some pupils may require additional teaching including reminders, prompts and further explanation to reinforce their existing knowledge and understanding of online safety issues.

Where a pupil has poor social understanding, careful consideration is given to group interactions when raising awareness of online safety. Internet activities are planned and well managed for these children and young people.

Online Safety Roles and Responsibilities

As Online Safety is an important aspect of strategic leadership within the school, the Headteacher and governors have ultimate responsibility to ensure that the policy and practices are embedded and monitored. The named Online Safety Coordinator in this school is Alison Harvey who has been designated this role as a member of the senior leadership team. The Online Safety Leader is Nicola Redden. All members of the school community have been made aware of who holds this post. It is the role of the Online Safety Coordinator to keep abreast of current issues and guidance through organisations such as West Northamptonshire LA, Becta, CEOP (Child Exploitation and Online Protection) and Childnet.

The Governors are updated by the Headteacher/ Online Safety Coordinator and all governors have an understanding of the issues and strategies at the school in relation to local and national guidelines and advice.

This policy, supported by the school's acceptable use agreements for staff, governors, visitors and pupils, is to protect the interests and safety of the whole school community. It is linked to the following mandatory school policies: safeguarding, health and safety, home–school agreements, and behaviour/pupil discipline (including the Anti-bullying) policy and PSHE.

Role	Key Responsibilities
Headteacher	• To ensure all staff are aware of dangers associated with electronic communication • To have a legal duty of care to ensure all pupils and staff are safe • To take overall responsibility for Online safety provision • To take overall responsibility for data and data security • To ensure the school uses an approved, filtered Internet Service, which complies with current statutory requirements - Securly

Role	Key Responsibilities
	• To be responsible for ensuring that staff receive suitable training to carry out their online safety roles and to train other colleagues, as relevant. • To be aware of procedures to be followed in the event of an Online Safety incident. • Access regular and appropriate training and support to ensure they understand the unique risks associated with online safety and have the relevant knowledge and up to date required to keep learners safe online. • To receive weekly monitoring reports each Monday, from the DSL/Online Safety leader/School Computing Technical Staff. • To ensure that there is a system in place to monitor and support staff who carry out internal online safety procedures.
Online Safety Co-ordinator / Online Safety leader (Dept DSL/ Designated Safeguarding Leader	• Takes day to day responsibility for online safety issues and has a leading role in establishing and reviewing the school Online Safety policies / documents (Online Safety 360 self-review) • Promotes an awareness and commitment to online safeguarding throughout the school community • Takes the lead on understanding the filtering and monitoring systems and processes in place on school devices and school networks without unreasonably impacting teaching and learning. • Liaises with school computing technical staff (Easi PC (Technical Support Service), Scott Kennedy (IT HLTA Support) and Scott Lagdon (Computing Lead)) to make sure appropriate systems and processes are in place • To communicate regularly with SLT and the designated Online Safety governor: Gary Palmer to discuss current issues, review incident logs and filtering / change control logs. • To ensure that all staff are aware of the procedures that need to be followed in the event of an online safety incident. • To ensure that an online safety incident log is kept up to date. • Facilitates training and advice for all staff. • Liaises with the Local Authority and relevant agencies • Are regularly updated in Online Safety issues and legislation, and be aware of the potential for safeguarding issues to arise from: • sharing of personal data • access to illegal / inappropriate materials • inappropriate on-line contact with adults / strangers • potential or actual incidents of grooming • cyber-bullying and use of social media.
Governors / Online safety governor	• To ensure that the school follows all current online safety advice to keep the children and staff safe

Role	Key Responsibilities
	• Review DfE filtering and monitoring systems and discuss with IT staff and EasiPC what needs to be done to support the school in meeting those standards, which include: - Identifying and assigning roles and responsibilities to manage filtering and monitoring systems; - Reviewing filtering and monitoring provisions at least annually; - Blocking harmful and inappropriate content without unreasonably impacting teaching and learning; - Having effective monitoring strategies in place that meet their safeguarding needs. • To approve the Online Safety policy and review the effectiveness of the policy. This will be carried out by the Governors receiving regular information about online safety incidents and monitoring reports. Gary Palmer has taken on the role of Online Safety governor. • To support the school in encouraging parents and the wider community to become engaged in Online Safety activities
Computing Curriculum Leader	• To oversee the continuous delivery of the online safety element of the computing curriculum alongside the Online Safety coordinator. • To liaise with the Online Safety coordinator regularly. • Ensures that Online Safety education is embedded across the curriculum
Network Manager/technician – EasiPC/school IT support	• To report any online safety related issues that arise, to the Online Safety Coordinator (Alison Harvey) or Online Safety leader (Nicola Redden). • To ensure that users may only access the school's networks through an authorised and properly enforced password protection • To ensure that provision exists for misuse detection and malicious attack e.g. keeping virus protection up to date • To ensure the security of the school IT system. • To ensure that access controls exist to protect personal and sensitive information held on school-owned devices. • The school's procedure on web filtering is applied and updated on a regular basis. • To keep up to date with the school's Online Safety policy and technical information in order to effectively carry out their online safety role and to inform and update others as relevant. • To ensure that the use of the network / remote access / email is regularly monitored in order that any misuse / attempted misuse can be reported to the Online Safety leader, Headteacher for investigation. • To work alongside the school to ensure appropriate backup procedures exist so that critical information and systems can be recovered in the event of a disaster. • To keep up-to-date documentation of the school's online security and technical procedures.
Data Manager	• To ensure that all data held on pupils on the school office machines have appropriate access controls in place.

Role	Key Responsibilities
Teachers	• To plan and teach focused online safety lessons at least termly. • To embed online safety issues in all aspects of the curriculum and other school activities. • To ensure all children are aware of their Acceptable Use Agreement. • To supervise and guide pupils carefully when engaged in learning activities involving online technology, including extra-curricular and extended school activities if relevant. • To ensure that pupils are fully aware of research skills, legal issues relating to electronic content such as copyright laws. • Educating pupils on the dangers of technologies that maybe encountered outside school is done informally when opportunities arise and as part of the Online Safety curriculum.
All staff	• To read, understand and help promote the school's Online Safety policies and guidance. • To read understand, sign and adhere to the school Acceptable Use Agreement and Policy. • To be aware of online safety issues related to the use of mobile phones, cameras and hand-held devices and that they monitor their use and implement current school policies with regard to these devices. • To report any suspected misuse or problem to the online safety coordinator • To maintain an awareness of current online safety issues and guidance e.g. through CPD • To model safe, responsible and professional behaviours in their own use of technology • To ensure that any digital communications with parents and pupils should be on a professional level and only through school-based systems, never through personal mechanisms, e.g. email, text, mobile phones etc.
Pupils	• Read, understand, sign and adhere to the Pupil Acceptable Use Policy. • Have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations. • To understand the importance of reporting abuse, misuse or access to inappropriate materials. • To know what action to take if they or someone they know feels worried or vulnerable when using online technology. • To know and understand school policy on the use of mobile phones, digital cameras and handheld devices. • To know and understand school policy on the taking / use of images and on cyber-bullying. • To understand the importance of adopting good online safety practice when using digital technologies out of school and realise that the school's Online Safety Policy covers their actions out of school, if related to their membership of the school.

Role	Key Responsibilities
	• To take responsibility for learning about the benefits and risks of using the Internet and other technologies safely both in school and at home.
Parents/carers	• To support the school in promoting online safety and endorse the Pupil Acceptable Use Agreement which includes the pupils' use of the internet • To give permission for school's use of photograph and video images. • To read, understand and promote the school Pupil Acceptable Use Agreement with their children • To consult with the school if they have any concerns about their children's use of technology.
External groups	• Any external individual / organisation will sign an Acceptable Use Policy prior to using any equipment or the Internet within school.

Communication:

The policy will be communicated to staff, pupils, governors and the community in the following ways:

- Policy to be posted on the school website.
- Policy to be part of school induction pack for new staff.
- Pupil Acceptable Use Agreements discussed with pupils at the start of each year and displayed in all classrooms.
- Staff Acceptable use agreements to be issued to whole school community, usually on entry to the school.

Handling complaints:

- The school will take all reasonable precautions to ensure online safety. However, owing to the international scale and linked nature of Internet content, the availability of mobile technologies and speed of change, it is not possible to guarantee that unsuitable material will never appear on a school computer or mobile device. Neither the school nor the Local Authority can accept liability for material accessed, or any consequences of internet access.
- Staff and pupils are given information about consequences for unacceptable use and possible sanctions. Sanctions available include:
    - Interview, counselling by teacher, Phase Leaders, Online Safety Coordinator / Headteacher.
    - Informing parents or carers.
    - Removal of internet or computer access for a period.
    - Referral to LA / Police
    - Accessing extremist material could result in a referral to 'Channel'.
- Our Online Safety Coordinator acts as first point of contact for any complaint. Any complaint about staff misuse is referred to the Headteacher.

- If the complaint is regarding the Headteacher, the Chair of Governors, Mary Kay (Acting Chair) should be contacted.
- Complaints of cyber-bullying are dealt with in accordance with our Anti-bullying policy. Complaints related to safeguarding are dealt with in accordance with school and LA child protection procedures as a maintained school.

The Curriculum:

Pupil Online Safety Curriculum

This school

- Has a clear, progressive online safety education program as part of the Computing curriculum (NCCE Teach Computing) and PSHE learning. It is built on the The Knowsley City Learning Centre Computing Scheme of Work for online safety, Jigsaw PSHE scheme of work and Education for a Connected World framework as advised in Teaching Online Safety in School (2019).
- Online safety is delivered from EYFS to Y6, which is adapted according to the needs of our pupils and the ever-changing world and being threaded through the PSHE curriculum. This covers a range of skills and behaviours appropriate to their age and experience, including:
    - To STOP and THINK before they CLICK.
    - To develop a range of strategies to evaluate and verify information before accepting its accuracy.
    - To be aware that the author of a website 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 or email, i.e. be polite, no bad or abusive language or other inappropriate behaviour; keep personal information private.
    - To understand how photographs can be manipulated and how web content can attract the wrong sort of attention.
    - To understand why online ‘friends’ may not be who they say they are and to understand why they should be careful in online environments.
    - 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 pictures 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.
    - In partnership with parents we will support pupils of an appropriate age to understand why and how some people will ‘groom’ young people for sexual reasons.

  - To understand the impact of online bullying, sexting, extremism 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 online bullying; 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

- The school plans internet use carefully to ensure that it is age-appropriate and supports the learning objectives for specific curriculum areas.
- It will remind students about their responsibilities through an Acceptable Use Agreement which is displayed throughout the school.
- It will ensure staff will model safe and responsible behaviour in their own use of technology during lessons.
- It will ensure that when copying materials from the web, staff and pupils understand issues around plagiarism; how to check copyright and also know that they must respect and acknowledge copyright / intellectual property rights.
- It will ensure that staff and pupils understand the issues around aspects of the commercial use of the Internet such as age appropriate internet use. This may include; risks in pop-ups, buying online, online gaming or gambling.

Staff and Governor Training

This school:

- Ensures staff know how to send or receive sensitive and personal data.
- Makes regular training available to staff on online safety issues and the school's online safety education program; provides annual updates and when needed due to changes in legislation.
- Provides, as part of the induction process, all new staff [including those on university/college placement and work experience] with information and guidance on the Online Safety policy and the school's Acceptable Use Agreement.

Supporting Parents

This school runs a rolling program of advice and guidance for parents, including:

- Introduction of the Acceptable Use Agreements to new parents, to ensure that principles of online safe behaviour are made clear.
- Monthly information newsletters
- Information webinars relating to online safety to provide guidance and advice for safe internet use at home.
- Provision of information about national support sites for parents.

Password policy

- This school makes it clear that staff and pupils must always keep their personal password private, must not share it with others and must not leave it where others can find it.
- All staff and children have their own unique username and private passwords to access school systems.
- We require staff to use STRONG passwords to ensure school information/data is kept safe using a 'complex' password.
-

e-Mail at Bridgewater Primary School

Staff e-Mail

The use of e-mail within most schools is an essential means of communication for both staff and pupils. In the context of school, e-mail should not be considered private. Educationally, e-mail can offer significant benefits including; direct written contact between schools on different projects, be they staff based or pupil based, within school or internationally. We recognise that pupils need to understand how to style an e-mail in relation to their age and good network etiquette; 'netiquette'. "Understand computer networks including the internet; how they can provide multiple services, such as the world wide web; and the opportunities they offer for communication and collaboration" (National Curriculum, 2013).

Managing e-Mail

- The school gives all staff their own e-mail account to use for all school business as a work based tool. This is to minimise the risk of receiving unsolicited or malicious e-mails and avoids the risk of personal profile information being revealed
- It is the responsibility of each account holder to keep the password secure and 'complex passwords' are encouraged. For the safety and security of users and recipients, all mail is filtered and logged; if necessary e-mail histories can be traced. The school email account should be the account that is used for all school business
- It is the responsibility of the Headteacher/Online Safety Coordinator (Alison Harvey) and the Online Safety Leader (Nicola Redden) to ensure the email accounts are maintained and are up to date.
- Under no circumstances should staff contact pupils, parents or conduct any school business using personal e-mail addresses.
- Documents that are sent as attachments containing data/personal information will be password protected.
- All e-mails should be written and checked carefully before sending, in the same way as a letter written on school headed paper.
- E-mails created or received as part of your school job will be subject to disclosure in response to a request for information under the Freedom of Information Act 2000. You must therefore actively manage your e-mail account as follows:
- Staff must inform Alison Harvey or Nicola Redden if they receive an offensive e-mail
- The use of Hotmail, BTInternet, AOL or any other Internet based webmail service for

sending, reading or receiving business related e-mail is not permitted. All staff use a school email address and Microsoft Outlook account.

Sending e-Mails

- If sending e-mails containing personal, confidential, classified or financially sensitive data to external third parties or agencies, refer to the section: e-mailing Personal, Sensitive, Confidential or Classified Information.
- Use your own school e-mail account so that you are clearly identified as the originator of a message.
- Keep the number and relevance of e-mail recipients, particularly those being copied, to the minimum necessary and appropriate.
- Do not send or forward attachments unnecessarily. Whenever possible, send the location path to the shared drive rather than sending attachments.
- An outgoing e-mail greater than ten megabytes (including any attachments) is likely to be stopped automatically. This size limit also applies to incoming e-mail.
- School e-mail is not to be used for personal advertising.

Receiving e-Mails

- Check your e-mail regularly
- Never open attachments from an untrusted source; consult with your network manager first
- Do not use the e-mail systems to store attachments. Detach and save business related work to the appropriate shared drive/folder

e-Mailing Personal, Sensitive, Confidential or Classified Information

- Assess whether the information can be transmitted by other secure means before using e-mail - e-mailing confidential data is not recommended and should be avoided where possible. Where essential, follow the school's procedure on encrypting data with a password.
- The use of Hotmail, BTInternet, AOL or any other Internet based webmail service for sending e-mail containing sensitive information is not permitted – again, the school's email accounts is the only exception.
- Where your conclusion is that e-mail must be used to transmit such data:
  - Obtain express consent from your manager to provide the information by e-mail
  - Exercise caution when sending the e-mail and always follow these checks before releasing the e-mail: Verify the details, including accurate e-mail address, of any intended recipient of the information Verify (by phoning) the details of a requestor before responding to e-mail requests for information

- Do not copy or forward the e-mail to any more recipients than is absolutely necessary
- Do not send the information to anybody/person whose details you have been unable to separately verify (usually by phone). Send the information as an encrypted document **attached** to an e-mail
- Provide the encryption key or password by a **separate** contact with the recipient(s); do not identify such information in the subject line of any e-mail.
- In exceptional circumstances, the County Council makes provision for secure data transfers to specific external agencies.

Pupil e-Mails

- Pupils may only use school approved accounts on the school system and only under direct teacher supervision for educational purposes
- All pupil e-mail users are expected to adhere to the generally accepted rules of etiquette particularly in relation to the use of appropriate language and not revealing any personal details about themselves or others in e-mail communication, or arrange to meet anyone without specific permission, and virus checking attachments.
- Pupils are introduced to e-mail as part of the Computing scheme of work
- Pupils must immediately tell a teacher/trusted adult if they receive an offensive e-mail and not delete any emails so to keep as evidence.

The School Website

- The Headteacher takes overall responsibility to ensure that the website content is accurate and the quality of presentation is maintained.
- Uploading of information is restricted to our website authorisers: e.g. Julie Breakwell (Office Manager), Michelle Martin (Finance Administrator) and Chris Elliott (website provider).
- The school web site complies with the statutory DfE guidelines for publications.
- Most material is the school's own work; where other's work is published or linked to, we credit the sources used and state clearly the author's identity or status.
- The point of contact on the web site is the school address, telephone number and a form, which is sent to the School Business Manager (Hilary Atlas), the relevant information is forwarded to the most appropriate member of staff. Home information or individual e-mail identities will not be published.
- Photographs published on the web do not have full names attached.
- We do not use pupils' names when saving images in the file names or in the tags when publishing to the school website.
- We do not use embedded geodata in respect of stored images.

- We expect teachers using school approved blogs or wikis to password protect them and run from the school website.

Social Media

Teachers are instructed not to run social network spaces for student use on a personal basis or to open up their own spaces to their students, but to use the school's preferred system for such communications.

- The school's system for social networking will be maintained in adherence with this policy. The school networking sites are updated and moderated by members of school staff.

School staff will ensure that in private use:

- They do not accept or request pupils as 'friends' on social networking sites or exchange personal email addresses or mobile phone numbers with students.
- They do not publish defamatory and /or false materials about Bridgewater Primary and Nursery School.
- No reference should be made in social media to students / pupils, parents / carers or school staff.
- They do not engage in online discussion on personal matters relating to members of the school community.
- Personal opinions should not be attributed to the school or local authority.
- Security settings on personal social media profiles are regularly checked to minimise risk of loss of personal information.
- Staff agree not to publish content that may be considered threatening, hurtful or defamatory to others and to consider the appropriateness of sharing specific and detailed private thoughts, concerns, images or messages on any social media services. Staff must have an awareness at all times of the school's digital footprint.

Online Hate

We will take all reasonable precautions to ensure that

- Online hate content, directed towards or posted by, specific members of the community will not be tolerated at Bridgewater Primary School and will be responded to in line with existing policies, including anti-bullying, safeguarding, the Equality Duty and behaviour.
- All members of the community will be advised to report online hate in accordance with relevant policies and procedures.
- The Police will be contacted if a criminal offence is suspected.
- If we are unclear on how to respond, or whether a criminal offence has been committed, the DSL (or deputy) will obtain advice through the Education Safeguarding Team and Northamptonshire Police.

Online Radicalisation and Extremism

Pupils should be supported in building resilience to radicalisation by providing a safe environment for debating controversial issues and helping them to understand how they can influence and participate in decision-making.

N.B.. The Counter Terrorism & Security Act 2015: The Act places a Prevent duty on specified schools to have "due regard to the need to prevent people from being drawn into terrorism". This duty is known as the Prevent duty. Schools must have regard to statutory guidance issued under section 29 of the CTSA 2015 ("the Prevent guidance"). The education and childcare specified authorities in Schedule 6 to the Act are as follows:

Schools/settings subject to the Prevent Duty will be expected to demonstrate activity in the following areas:

- Assessing the risk of children being drawn into terrorism
- Demonstrate that they are protecting children and young people from being drawn into terrorism by having robust safeguarding policies.
- Ensure that their safeguarding arrangements take into account the policies and procedures of the Local Safeguarding Children Board.
- Make sure that staff have training that gives them the knowledge and confidence to identify children at risk of being drawn into terrorism, and to challenge extremist ideas which can be used to legitimise terrorism
- Expected to ensure children are safe from terrorist and extremist material when accessing the internet in school
- Learners and staff are safe from terrorist and extremist material when accessing the internet on site.
- If we are concerned that a child or parent/carer may be at risk of radicalisation online, the DSL (or deputy) will be informed immediately, and action will be taken in line with our Safeguarding policy.
- If we are concerned that a member of staff may be at risk of radicalisation online, the Headteacher will be informed immediately, and action will be taken in line with the Safeguarding, Whistleblowing and NCC Allegations policies.

Equipment and Digital Content

Personal mobile phones and mobile devices

- Mobile phones brought into school are entirely at the staff member, student's (Upper KS 2 only) and 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.
- Student mobile phones which are brought into school must be turned off (not placed on silent) and stored in a designated area out of children's reach. They must remain turned off and out of sight until the end of the day. Student devices should not be used on the school premises.
- Parents/carers and visitors (including volunteers and contractors) must not use their mobile phones and personal devices on site, in accordance with our acceptable use policy.

- Staff are advised to use passwords/pin numbers to ensure that unauthorised calls or actions cannot be made on their phones or devices; passwords and pin numbers should be kept confidential and mobile phones and personal devices should not be shared.
- 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 or unacceptable use, 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 in the PPA room and staff room. 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 from the Headteacher to use their phone at other than their break times.
- Mobile phones and personally-owned devices will not be used in any way during lessons or formal school time (unless authorised by the Headteacher) or within toilet or changing areas. They should be switched off or silent at all times.
- Additionally, for all staff, all mobile phones, cameras and other electronic devices with imaging and sharing capabilities for staff and visitors are kept locked away in a cupboard Early years foundation stage profile: 2024 handbook (publishing.service.gov.uk).
- During school outings staff will have access to a school mobile / personal phone (if authorised by the Headteacher) which can be used for emergency contact purposes.
- It is the responsibility of the adult to ensure that there is no illegal or inappropriate content stored on their device when brought onto the school grounds.
- Personal mobile phones should never be used to contact children, young people or their families, apart from in exceptional circumstances, such as in an emergency on a school trip. Where this is the case, staff will block their number by dialing 141 before the phone number.
- Personal devices should not be used to take videos or photographs of the children. However, in exceptional circumstances, such as equipment shortages on a trip, permission may be granted by the Headteacher, provided there is an agreed timescale for transfer and deletion of the image from the staff member's device.

Students' use of personal devices

- Many personal devices have unlimited and unrestricted access to the internet via mobile phone networks (i.e. 3G, 4G and 5G). This access means that some children, whilst at school, can engage in inappropriate activities e.g. access harmful content, bully, harass or take digital images/ videos of themselves or others.
- The School accepts that there may be particular circumstances in which a parent wishes their child to have a mobile phone for their own safety e.g. when walking home. For this reason, children in Year 5 and Year 6 will be allowed to bring mobile phones to school. Phones must not be used when on the school premises.
- On entry to school, phones must be turned off (not placed on silent), handed in to class teachers on arrival in class so they can be stored in a designated area out of children's

reach until the end of the day. Spot-checks may be completed to ensure procedures are followed.

- If a student breaches the school policy and guidelines are broken, phones will be taken and stored centrally in the school office and will be returned at the end of the day. The phones should remain turned off until the children exit the school gate. Parents will be invited to school to discuss any breaches and subsequent consequences.
- Phones and devices must not be taken into examinations or statutory assessments.
- If a student needs to contact his or her parents or carers, they will be allowed to use a school phone. Parents are advised not to contact their child via their mobile phone during the school day, but to contact the school office.
- Tablets/smart watches/wearable technology are not permitted in school.

Digital images and video

In this school:

- We gain parental / carer permission for use of digital photographs or video involving their child as part of the school agreement form when their daughter or son joins the school.
- We do not identify pupils in online photographic materials or include the full names of pupils in the credits of any published school produced video materials / DVDs.
- We ask parents to ensure that any photographs taken at productions are kept purely for personal use and not uploaded to social media or sent on to others. Parents are reminded of this at the start of any production or event.
- We encourage parents to be mindful of their own use of mobile phones around school at events such as Termly Learning Conferences and Sports Days to act as good role models to their children and be 'present' in their learning.
- The school blocks/filters access to social networking sites or newsgroups unless there is a specific approved educational purpose.
- Pupils are taught about how images can be manipulated in their Online Safety education program and also taught to consider how to publish for a wide range of audiences which might include governors, parents or younger children as part of their ICT scheme of work.
- Pupils are taught that they should not post images or videos of others without their permission. We teach them about the risks associated with providing information with images (including the name of the file), that reveals the identify of others and their location, such as house number, street name or school. We teach them about the need to keep their data secure and what to do if they are subject to bullying or abuse.
- Pupils are not permitted to use personal digital equipment, including mobile phones and cameras, to record images of others; this includes when on field trips.

Generative artificial intelligence (AI)

Artificial intelligence (AI) tools are now widespread and easy to access. Staff, pupils and parents/carers may be familiar with generative chatbots such as ChatGPT and Google Bard.

Bridgewater recognises that AI has many uses to help pupils learn but may also have the potential to be used to bully others. For example, in the form of 'deepfakes', where AI is used to create images, audio or video hoaxes that look real.

We will treat any use of AI to bully pupils in line with our anti-bullying and behaviour policies.

Managing the IT and computing infrastructure

Internet access, security, virus protection, filtering and monitoring

This school:

- Has the educational filtered secure broadband connectivity through Securly.

- Uses the Securly filtering system which blocks sites that fall into categories such as pornography, race hatred, gaming, sites of an illegal nature, etc. All changes to the filtering policy are logged and only available to staff with the approved 'web filtering management' status.

- Uses Securly user-level filtering for all devices through both extension and DNS based filtering.

- The school use Securly Aware as its monitoring systems

- Ensures network health through use of Webroot anti-virus software from IT Support Provider etc. and network set-up so staff and pupils cannot download executable files.

- Uses a DfE, LA approved system, Microsoft SharePoint using encrypted password protected links. All devices are encrypted using Bitlocker to protect data whilst offsite. Blocks all chat rooms and social networking sites except those that are part of an educational network or approved Learning Platform.
    - Only unblocks other external social networking sites for specific purposes such as Internet Literacy lessons.
    - Has blocked pupil access to music download or shopping sites, except those approved for educational purposes at a regional or national level.
    - Uses security time-outs on internet access where practicable and useful.
    - Works in partnership with IT support provider and Securly to ensure any concerns about the system are communicated so that systems remain robust and protect students.

- Is vigilant in its supervision of pupils' use at all times, as far as is reasonable, and uses common-sense strategies in learning resource areas where older pupils have more flexible access.
- Ensures all staff and students have signed an acceptable use agreement form and understands that they must report any concerns.
- Ensures pupils only publish within an appropriately secure environment the school's learning environment.
- Requires staff to preview websites before use and direct students to subject and age appropriate web sites and uses child-friendly search engines where more open internet searching is required.
- Is vigilant when conducting 'raw' image search with pupils e.g. Google image search.
- Informs all users that internet use is monitored.
- Informs staff and students that that they must report any failure of the filtering systems directly to the online safety officer so they can be logged or escalated by our system administrator to the Technical service provider or EXA Helpdesk as necessary.
- Makes clear all users know and understand what the 'rules of appropriate use' are and what sanctions result from misuse through staff meetings and teaching programs.
- Provides advice and information on reporting offensive materials, abuse/ bullying etc. available for pupils, staff and parents.
- Immediately refers any material we suspect is illegal to the appropriate authorities - Police and the LA.

- **Network management (user access, backup)**

  This school
  - Uses individual, audited log-ins for all users.
  - Uses guest accounts occasionally for external or short-term visitors for temporary access to appropriate services.
  - Ensures the Systems Administrator is up-to-date with services and policies.
  - Storage of all data within the school will conform to the UK data protection requirements.

To ensure the network is used safely, this school:

- Ensures all staff read and sign that they have understood the school's Online Safety Policy. Following this, they are set-up with internet, email access and network access. Online access to service is through a unique, audited username and password. We also use the same username and password for access to our school's network.
- Staff access to the school's management information system is controlled through a separate password for data security purposes.
- We provide pupils with an individual network log-in username. From Year 2 they are also expected to use a personal 'complex' password.
- Makes clear that no one should log on as another user and makes clear that pupils should never be allowed to log-on or use teacher and staff logins as these have far less security restrictions and inappropriate use could damage files or the network.
- Has set-up the network with a shared work area for pupils and one for staff. Staff and pupils are shown how to save work and access work from these areas.
- Where a user finds a logged-on machine, we require them to always log-off and then log-on again as themselves.

- If a member of staff is leaving a computer unattended at any times of the day, they are required to lock the screen to ensure that laptops require a password to be used.
- Requests that teachers DO switch the computers off at the end of the day.
- Has set-up the network so that pupils cannot download executable files / programs.
- Has blocked access to music/media download or shopping sites – except those approved for educational purposes.
- Scans all mobile equipment with anti-virus / spyware before it is connected to the network.
- Makes clear that staff are responsible for ensuring that all equipment that goes home has the anti-virus and spyware software maintained up-to-date and the school provides them with a solution to do so.
- Makes clear that staff are responsible for ensuring that any computer or laptop loaned to them by the school, is used solely to support their professional responsibilities and that they notify the school of any "significant personal use" as defined by HM Revenue & Customs.
- Makes clear that staff accessing LA systems do so in accordance with any Corporate policies; e.g. LA egress email or Intranet; finance system, Personnel system etc.
- Maintains equipment to ensure Health and Safety is followed.
- Has integrated curriculum and administration networks, but access to the Management Information System is set-up so as to ensure staff users can only access modules related to their role.
- Ensures that access to the school's network resources from remote locations by staff is restricted and access is only through school / LA approved systems: *e.g. teachers access their area / a staff shared area for planning documentation via a VPN solution / RAv3 system.*
- Does not allow any outside Agencies to access our network remotely except where there is a clear professional need and then access is restricted and is only through approved systems. e.g. technical support or MIS Support, our Education Welfare Officers accessing attendance data on specific children, parents using a secure portal to access information on their child.
- Provides pupils and staff with access to content and resources through the website which staff access using their username and password.
- Makes clear responsibilities for the daily back up of MIS and finance systems and other important files.
- Has a clear disaster recovery system in place for critical data that includes a secure, remote back up of critical data that complies with external Audit's requirements.
- Uses the DfE secure s2s website for all CTF files sent to other schools.
- Ensures that all pupil assessment data or personal data sent over the Internet is encrypted or only sent within the approved secure system in our LA or through USO secure file exchange USO FX.
- Follows ISP advice on Local Area and Wide Area security matters and firewalls and routers have been configured to prevent unauthorised use of our network.
- Our wireless network has been secured to industry standard Enterprise security level /appropriate standards suitable for educational use.
- All computer equipment is installed professionally and meets health and safety standards.

- Smartboards and interactive whiteboards are maintained so that the quality of presentation remains high.
- Reviews the school IT systems regularly with regard to health and safety and security.

Data security: Management Information System access and Data transfer

Strategic and operational practices

At this school:

- We ensure staff know who to report any incidents where data protection may have been compromised.
- All staff are DBS checked and records are held in one central record.
- We require that any Protect and Restricted material must be encrypted if the material is to be removed from the school and limit such data removal. We have an approved remote access solution so staff can access sensitive and other data from home, without need to take data home.
- School staff with access to setting-up usernames and passwords for email and network access are working within the approved system and follow the security processes required by those systems.

Technical Solutions

- Staff have secure area on the network and Microsoft 365 to store sensitive documents or photographs.
- We use the AVCO to securely transfer CTF pupil data files to other schools in Northamptonshire.
- We also use S2S to securely transfer CTF pupil data files to other schools out of the country.
- We use RAv3 / VPN solution with its 2-factor authentication for remote access into our systems.
- We store any Protect and Restricted written material in lockable storage cabinets.
- All servers are in lockable locations and managed by DBS-checked staff.
- We lock any back-up tapes in a secure, fire-proof cabinet. No back-up tapes leave the site on mobile devices.
- We comply with the WEEE directive on equipment disposal by using an approved or recommended disposal company for disposal of equipment where any protected or restricted data has been held and get a certificate of secure deletion for any server that once contained personal data.
- Portable equipment loaned by the school for use by staff at home, where used for any protected data, is disposed of through the same procedure.
- Paper based sensitive information is shredded or put into confidentiality waste which is collected by a secure data disposal service.
- Any device being disposed of should go to a reputable company who will provide the school with a data destruction certificate.

Asset disposal

- Details of all school-owned hardware will be asset tracked.
- 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. The school will only use authorised companies who will supply a written guarantee that this will happen
- Disposal of any equipment will conform to The Waste Electrical and Electronic Equipment Regulations 2006 and/or The Waste Electrical and Electronic Equipment (Amendment) Regulations 2007. Further information can be found on the Environment Agency website.

Incident Reporting

Online Safety Incident Log and Infringements

Any security breaches or attempts, loss of equipment and any unauthorised use or suspected misuse of ICT must be immediately reported to the Headteacher or Online Safety Coordinator. Additionally, all security breaches, lost/stolen equipment or data (including remote access SecureID tokens and PINs), virus notifications, unsolicited emails, misuse or unauthorised use of ICT and all other policy non-compliance must be reported to the Headteacher and/or the Online Safety Coordinator.

Expected Conduct and Incident management:

Expected conduct

In this school, all users:

- Are responsible for using the school computing systems in accordance with the relevant Acceptable Use Agreement which they will have been taught, which will be recapped annually.
- Need to understand the importance of misuse or access to inappropriate materials and are aware of the consequences.
- Need to understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so.
- Should understand the importance of adopting good online safety practice when using digital technologies out of school and realise that the school's Online Safety Policy covers their actions out of school, if related to their membership of the school.
- Will be expected to know and understand school policies on the use of mobile phones, digital cameras and hand-held devices. They should also know and understand school policies on the taking / use of images and on online bullying.

Staff

- Are responsible for reading the school's Online Safety Policy and using the school computing systems accordingly, including the use of mobile phones, and hand-held devices.

Students/Pupils

- Should have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations

Parents/Carers

- Should provide consent for pupils to use the Internet, as well as other technologies, as part of the Online Safety Acceptable Use Agreement form at time of their child's entry to the school.
- Should know and understand what the 'rules of appropriate use' are.

Inappropriate Material

All users are aware of the procedures for reporting accidental access to inappropriate materials. The breach must be immediately reported to the Online Safety Coordinator.

Deliberate access to inappropriate materials by any user will lead to the incident being logged by the Online Safety Coordinator, depending on the seriousness of the offence; investigation by the Headteacher/ LA, immediate suspension, possibly leading to dismissal and involvement of police for very serious offences.

Incident Reporting Procedure:

- If an incident is reported to a member of staff it needs to be reported to the DSLs and Online Safety Leader and logged.
- The child/children and/or all parties involved should be spoken with (if appropriate) to gain a full and fair understanding of the incident.
- If appropriate the child / children will be referred to the child friendly Online Safety Acceptable Use Agreement and/or the Anti-bullying Policy.
- Staff will record concerns on My Concern and also discuss concerns directly with the Headteacher/Online Safety Coordinator, Online Leader and the Designated Senior Leader for Safeguarding: Frances Troop (DHT).
- Either the class teacher or the Online Safety leader (depending on the incident) will make contact with the parents/carers if appropriate.
- Outside agencies will be involved when appropriate e.g. the LA, police, CEOP, Simon Aston (Northampton Online Safety officer, possibly liaise with other schools)
- The incident is then discussed and next steps agreed to put in any consequences if appropriate and /or to provide support for children involved to ensure they understand Online Safety regulations and reiterate Online Safety rules set out by the school following the National Guideline.
- Historic incident logs are all locked in a secure cupboard.

Policy updated September 2023

Policy next reviewed September 2024

Staff, Governor and Visitor
Acceptable Use Agreement / Code of Conduct

ICT (including data) and the related technologies such as e-mail, the internet and mobile devices are an expected part of our daily working life in school. The Online Safety policy is designed to ensure that all staff are aware of their professional responsibilities when using any form of ICT. All staff are expected to sign to say they have read this policy and adhere at all times to its contents, as well as the key points restated below. Any concerns or clarification should be discussed with Nicola Redden, Alison Harvey or Frances Troop.

- I will only use the school's email / Internet and any related technologies for professional purposes or for uses deemed acceptable 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, personal e-mail address, personal Twitter account, or any other social media link, to pupils and will not request or add pupils as 'friends' on social media.
- I will only use the approved, secure e-mail system(s) for any school business.
- I will ensure that personal data 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. Personal or sensitive data taken off site must be encrypted, e.g. on a password secured laptop or memory stick.
- 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 in line 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 Headteacher.
- I will support the school approach to online safety and not upload or add any images, video, sounds or text linked to or associated with the school or its community.
- 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, to my Line Manager or Headteacher.
- I will respect copyright and intellectual property rights.
- I will ensure that my online activity, both in school and outside of school, will not bring the school, my professional reputation, or that of others, into disrepute.
- I will support and promote the school's Online Safety policy and help pupils to be safe and responsible in their use of ICT and related technologies.
- I will not use personal electronic devices (including smart watches) in public areas of the school between the hours of 8.30am and 3.30pm, except in the staff room and PPA room and where there are signs to indicate this.
- I will immediately report any illegal, inappropriate or harmful material or incident, I become aware of, to the appropriate person.

User Signature

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

Signature …….……………………….………… Date ……………………

Full Name ………………………………….......................................(printed)

Job title ……………………………………………………………………

This agreement can be signed at the school office upon arrival to the school.

BRIDGEWATER PRIMARY SCHOOL

Early Years and Year 1 Online Safety Rules

I will stay on the game or app my grown up has chosen.

I will not click on an advert or pop up screen in a game.

I know that if I see something that makes me feel unsafe I need to switch it off, close the laptop, turn the phone or iPad over and put it down.

I will tell a grown up if I see a picture or message that makes me feel unsafe.

I will not send a picture or message that is unkind.

I will not send a message back if someone tries to talk to me online.

CLICK CEOP
Internet Safety

Year 2 to Year 6
Acceptable Use Agreement

Our Online Safety Rules

- **I will only use ICT in school for school purposes.**
- **I will only use my class e-mail address or my own school e-mail address when e-mailing.**
- **I will only open e-mail attachments from people I know, or who my teacher has approved.**
- **I will not tell other people my ICT passwords.**
- **I will only open/delete my own files.**
- **I will make sure that all ICT contact with other children and adults is responsible, polite and sensible, both in and out of school.**
- **I will not deliberately look for, save or send anything that could be unpleasant or nasty. If I accidentally find anything like this, I will tell my teacher immediately.**
- **I will not give out my own details such as my name, phone number or home address. I will not arrange to meet someone unless this is part of a school project approved by my teacher and a responsible adult comes with me.**
- **I will be responsible for my behaviour when using ICT because I know that these rules are to keep me safe.**
- **I will support the school approach to online safety and not deliberately upload or add any images, video, sounds or text that could upset any member of the school community**
- **I know that my use of ICT can be checked and that my parent/ carer contacted if a member of school staff is concerned about my online safety.**

Parent/Carer Online Safety Acceptable Use Agreement

Digital technologies have become integral to the lives of children and young people, both within school and outside school. These technologies provide powerful tools, which open up new opportunities for everyone. They can stimulate discussion, promote creativity and stimulate awareness of context to promote effective learning. Young people should have an entitlement to safe internet access at all times.

This Acceptable Use Agreement is intended to ensure:

- that young people will be responsible users and stay safe whilst online and when using any technology for educational, personal and recreational use
- that school systems and users are protected from accidental or deliberate misuse that could put the security of the systems and users at risk
- that parents and carers are aware of the importance of online safety and are involved in the education and guidance of young people with regard to their online behaviour

The school will try to ensure that pupils will have good access to digital technologies to enhance their learning and will, in return, expect the pupils to agree to be responsible users. A copy of the Pupil Acceptable Use Agreement is available in school, so that parents will be aware of the school expectations of the children.

Parents are requested to sign the permission form overleaf to show their support of the school's online safety procedures.

Permission Form

As the parent of the pupil named overleaf, I give permission for my son/daughter to have access to the internet and to ICT systems at school.

I understand that the school has discussed the Acceptable Use Agreement with my son/daughter and that they have and will receive continuous, online safety education to help them understand the importance of safe use of technology and the internet – both in and out of school.

I understand that the school will take every reasonable precaution, including monitoring and filtering systems, to ensure that young people will be safe when they use the internet and ICT systems. I also understand that the school cannot ultimately be held responsible for the nature and content of materials accessed on the internet and using mobile technologies.

I understand that my son's/daughter's activity on the ICT systems will be monitored and that the school will contact me if they have concerns about any possible breaches of the Acceptable Use Agreement.

I will reinforce the schools Acceptable Use Agreement at home and ensure my child fully understands the importance of following these online safety rules.

I will encourage my child to adopt safe use of the internet and digital technologies at home and will inform the school if I have concerns over my child's online safety.

I understand that Year 5 and Year 6 children may bring a mobile phone, but these cannot be used when on the school site. Phones will be handed in to class teachers on arrival in school and returned at the end of the day.

I understand that smart watches/fitness trackers are not permitted to be worn or used in school.

Use of Microsoft 365 Permission Form

The school uses Microsoft 364 apps and services for pupils and staff. This permission form describes the tools and pupil responsibilities for using these services.
The following services through Microsoft Office Suite are available to each pupil in school:

Microsoft 365 apps and services
Access - data base program
Excel - spreadsheet program
Teams - a communication and collaboration platform (emails managed by the school)
OneDrive - file hosting service
OneNote – note-taking program
Outlook – personal information
Publisher - a desktop publishing program
Powerpoint - presentation program
Word - word processing program

Using these tools, pupils collaboratively create, edit and share files and websites for school related projects and communicate via email with other pupils and members of staff. These services are entirely online and available 24/7 from any Internet-connected computer. Examples of student use include showcasing class projects, building an electronic portfolio of school learning experiences, and working in small groups on presentations to share with others. The school believes that use of the tools significantly adds to your child's educational experience.

As part of Microsoft 365 Terms and Conditions we are required to seek your permission for your child to have an account to access these:

As the parent of the pupil mentioned below, I agree to my child using the Microsoft 365 apps and services in school. Yes/No

Signed (Parent/Carer) Date:

Please print your name:

Name of child: Class teacher:

Letter to inform parents of children discussing use of PEGI age restricted games:

Bridgewater Primary School

Dear Parent/Carer,

Video Games and keeping your child safe:
Online Safety - key information for parents/carers

Child's name: ________________________________ Class: ___________

It has been brought to our attention that your child has been playing console games such as GAME NAME, even though the certification for this game is **18** based on International PEGI ratings

Bridgewater Primary School is committed to keeping our children safe and to promoting the safe, responsible use of the technologies. As such, we feel it is our responsibility to raise this particular issue as a concern.

1) Ratings denote the content and appropriateness of games
Since 2003 games have been age rated under the Pan-European Game Information (PEGI) system which operates in the UK and over 30 other countries of Europe, in addition, where a game showed realistic scenes of gross violence or sexual activity the game had to be legally classified and received one or other of the BBFC classification certificates given for videos/DVDs

3
www.pegi.info
7
www.pegi.info
12
www.pegi.info
16
www.pegi.info
18
www.pegi.info

The PEGI system has been effectively incorporated into UK law and video games will be age rated at one or other of the following age levels; which you will find on video game sleeves. Ratings do not denote the difficulty or the enjoyment level of a game, but that that it contains content suitable for a certain age group and above

The PEGI age ratings will enable parents and carers to make an informed choice when buying a game for their children.

It is important to note that the age ratings 12, 16 and 18 age ratings are mandatory and that it is **illegal** for a retailer to supply any game with any of these ratings to anyone below the specified age. The age ratings 3 and 7 are advisory only.

An 18 Rated game is applied when the level of violence reaches a stage where it becomes gross violence and/or includes elements of specific types of violence. **In general terms it is where the level of violence is so visually strong that it would make the reasonable viewer react with a sense of revulsion.**

This rating is also applied where the level of sexual activity is explicit which may mean that genitals are visible. Any game that glamorises the use of real-life drugs will also

probably fall into this category.

2) Content Indicators

BAD LANGUAGE
DISCRIMINATION
DRUGS
FEAR
GAMBLING
ONLINE
SEX
VIOLENCE

In addition to age ratings, video games will include indicators of the type of content and activities that the game includes in it.

The descriptors are fairly self-explanatory but should be read in conjunction with the age rating given for a video game.

A violence descriptor with an 18 rated game will indicate a more extreme level of violence than a violence descriptor with a 12 rated game. Similarly a sex/nudity descriptor with a 12 rated game will probably indicate sexual innuendo but a sex/nudity descriptor with an 18 rated game will indicate sexual content of a more explicit nature.

3) Parental responsibility

We feel it is important to point out to parents the risks of underage use of such video games, so **you** can make an *informed* decision as to whether to allow your child to be subjected to such images and content.

- The PEGI ratings system helps you make informed decisions about which video games to choose for your family
- A PEGI rating gives the suggested minimum age that you must be to play a game due to the suitability of the content
- As parents you can take direct control of what games your children play at home, how they play them and for how long through parental controls on video game systems such as the Xbox or Playstation
- Choosing and playing video games as a family is the best way to understand and enjoy them together
- The stories, worlds and characters in video games offer playful ways to engage with a wide range of subjects and fuels creativity, interests and imagination
- The recently re-launched askaboutgames.com website provides further information about video games ratings and offers real family stories and suggestions on how video games can be a creative and collaborative experience for all the family
- We also recommend that all parents visit the CEOP Think U Know website for more information on keeping your child safe online www.thinkuknow.co.uk

4) School support and action

Bridgewater Primary School is dedicated to ensuring pupils remain safe online. Each year all pupils have at least termly dedicated Online Safety lessons, alongside discussing Online Safety issues throughout the year as required. We also provide annual Online Safety workshops for parents. Alternatively, if you feel that you, or your child, need further support in keeping your child safe on the internet, please make an appointment to see Nicola Redden (Online Safety Lead).

Because of our duty to all the children in our school, we will take action (which may involve the police) if a problem comes to our attention that involves the safety or wellbeing of any of our pupils.

With thanks for your continued support,
Mrs Harvey
Headteacher