Draft

Bridgewater Primary School
Online Safety Policy

Reviewed 2016

ICT in the 21st Century is seen 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.

Information and Communications Technology 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
- Mobile/ Smart phones with text, video and/ or web functionality
- Other mobile devices with web functionality

Whilst exciting and beneficial both in and out of the context of education, much ICT, particularly web-based resources, are not consistently policed. All users need to be aware of the range of risks associated with the use of these Internet technologies.

Bridgewater Primary 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 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, in and beyond the context of the classroom.

Schools hold personal data on learners, staff and other people to help them conduct their day-to-day activities. Some of this information is sensitive and could be used by another person or criminal organisation to cause harm or distress to an individual. The loss of sensitive information can result in media coverage, and potentially damage the reputation of the school. This can make it more difficult for your school to use technology to benefit learners.

Everybody in the school has a shared responsibility to secure any sensitive information used in their day-to-day professional duties and even staff not directly involved in data handling should be made aware of the risks and threats and how to minimise them.

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 and staff, but brought onto school premises (such as laptops, mobile phones, camera phones, 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 School with respect to the use of IT-based technologies.
- Safeguard and protect the children and staff of Bridgewater Primary School.
- Assist school staff working with children to work safely and responsibly with the Internet and other communication technologies and to monitor their own standards and practice.
- Set clear expectations of behaviour and/or codes of practice relevant to responsible use of the Internet for educational, personal or recreational use.
- Have clear structures to deal with online abuse such as 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 enabling them to keep safe.
- Minimise the risk of misplaced or malicious allegations made against adults who work with students.

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: how to check authenticity and accuracy of online content

Contact

- grooming
- 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))
- sexting (sending and receiving of personally intimate images) also referred to as SGII (self-generated indecent images)
- extremism
- copyright (little care or consideration for intellectual property and ownership – such as music and film)

(Ref Ofsted 2013)

Scope:

This policy applies to all members of Bridgewater Primary School community, including staff, students, pupils, volunteers, parents, carers, visitors, community users etc. who have access to and are users of Bridgewater Primary School computing systems, both in and out of Bridgewater Primary School.

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 online bullying, or other online safety incidents covered by this policy, which may take place outside the Bridgewater Primary School but is linked to membership of Bridgewater Primary 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 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: Child Protection and Safeguarding 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 Safegauarding Leader (DSL) alongside the Online Safety coordinator and Child protection Officer 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 1998, the Human Rights Act 1998, the Regulation of Investigatory Powers Act 2000 (RIPA) and the Lawful Business Practice Regulations 2000.

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 NCC 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 SecureID tokens and PINs), virus notifications, unsolicited emails, misuse or unauthorised use of ICT and all other policy non-compliance must be reported to Headteacher or Online Safety Coordinator.

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 you what actions to take and be responsible for advising others that need to know.

Equal Opportunities 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.

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. This 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 this policy and adhere at all times to its contents. Any concerns or clarification should be discussed with Jenna Cox, 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.
- 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, eg 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 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 where there are signs to indicate this.

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.

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.
- 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 eSafety.
- I understand how to report abuse online using the click CEOP

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 attached to this permission form, so that parents/carers will be aware of the school expectations of the young people in their care.
Parents are requested to sign the permission form below to show their support of the school in this important aspect of the school's work.

Permission Form

As the parent/carer of the pupil named below, 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 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.

Signed (Parent/Carer) _____ Date: _____

Please print your name: _____ Name of child: _____

Use of Cloud Systems Permission Form

The school uses Google Apps for Education for pupils and staff. This permission form describes the tools and pupil responsibilities for using these services.

The following services are available to each pupil and hosted by Google as part of the school's online presence in Google Apps for Education:

GMail - school email accounts managed by the school
Google Calendar - an individual calendar providing the ability to organise schedules, daily activities and assignments
Google Docs - a word processing tool
Google Sheets - a spreadsheet tool
Google Slides - a presentation tool
Google Forms - a questionnaire building tool
Google Sites - an individual and collaborative website creation tool

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 the Google terms and conditions we are required to seek your permission for your child to have a Google Apps for Education account:

As the parent/carer of the above pupil, I agree to my child using the school using Google Apps for Education. **Yes/No**

Signed (Parent/Carer) _____ Date: _____

Please print your name: _____ Name of child: _____

Online Safety Roles and Responsibilities

As Online Safety is an important aspect of strategic leadership within the school, the Head 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/Jenna Cox who has been designated this role as a member of the senior leadership team. 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 Northamptonshire LA, Becta, CEOP (Child Exploitation and Online Protection) and Childnet.

Senior Management and Governors are updated by the Head/ Online Safety Coordinator and all governors have an understanding of the issues and strategies at our 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: child protection, 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 (SIRO) • To ensure the school uses an approved, filtered Internet Service, which complies with current statutory requirements; Surf Protect Fusion filtering via the ISP, EXA Education • 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. • To receive regular monitoring reports from the online Safety Co-ordinator / teachers. • 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 / Designated Child Protection Lead	• Takes day to day responsibility for online safety issues and has a leading role in establishing and reviewing the school Online Safety Policies / documents
	• Promotes an awareness and commitment to online safeguarding throughout the school community
	• Ensures that Online Safety education is embedded across the curriculum
	• Liaises with school computing technical staff
	• To communicate regularly with SLT and the designated online safety Governor: (Michael Montgomery) committee 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
	• Is regularly updated in Online Safety issues and legislation, and be aware of the potential for serious child protection 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
	  • online bullying and use of social media

Role	Key Responsibilities
Governors / Online safety governor	• To ensure that the school follows all current online safety advice to keep the children and staff safe • 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. Michael Montgomery 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 • The role of the Online Safety Governor will include regular reviews with the Online Safety Co-ordinator (including Online safety incident logs, filtering / change control logs)
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.
Network Manager/technician – EasiPC Russell Smith	• To report any online safety related issues that arise, to the Online Safety Coordinator (Jenna Cox). • To ensure that users may only access the school's networks through an authorised and properly enforced password protection policy, in which passwords are regularly changed • 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. • 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 Co-ordinator, 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.
Teachers	• To plan and teach focused online safety lessons 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 Acceptabe 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 pupils should be on a professional level

Role	Key Responsibilities
	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 hand held 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. • 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 Parent's Acceptable Use Agreement which includes the pupils' use of the internet and the 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 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.
- Acceptable use agreements discussed with pupils at the start of each year and displayed in all classrooms.
- Acceptable use agreements to be issued to whole school community, usually on entry to the school.
- Acceptable use agreements to be held in pupil and personnel files.

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, should be contacted.
- Complaints of online bullying are dealt with in accordance with our Anti-Bullying Policy. Complaints related to child protection are dealt with in accordance with school, LA child protection procedures

The Curriculum:

Pupil Online Safety Curriculum

This school

- Has a clear, progressive online safety education programme as part of the Computing curriculum and PSHE learning. It is built on the 'Rising Stars' scheme of work delivered from EYFS to Y6, which is adapted according to the needs of our pupils and the ever changing world. 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; keeping personal information private.
    - To understand how photographs can be manipulated and how web content can attract the wrong sort of attention.
    - To understand why 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 or the CLICK CEOP button.

- 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; 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 programme of advice, guidance and training for parents, including:
- Introduction of the Acceptable Use Agreements to new parents, to ensure that principles of online safe behaviour are made clear.
- Information leaflets; in school newsletters; on the school web site.
- Demonstrations, practical sessions held at school.
- Suggestions 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 have their own unique username and private passwords to access school systems. Staff are responsible for keeping their password private.
- 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 (Alison Harvey) and the Online Safety Coordinator (Jenna Cox) 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.

- All e-mails should be written and checked carefully before sending, in the same way as a letter written on school headed paper.
- Staff sending e-mails to external organisations, parents or pupils are advised to cc. the Headteacher or designated Online Safety Coordinator.
- 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 Jenna Cox 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.

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
- The automatic forwarding and deletion of e-mails is not allowed

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 Google 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 any body/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, request confirmation of safe receipt
- 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, 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 to 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. Jan Cox (Office Manager), 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 bursar (Theresa De La Fuente), 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 schools' 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:

- 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.

Equipment and Digital Content

Personal mobile phones and mobile devices

- Mobile phones brought into school are entirely at the staff member, student's & 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 designated area out of children's reach. They must remain turned off and out of sight until the end of the day. Staff members may use their phones during school break times.
- All visitors are requested to keep their phones on silent.
- 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. If a staff member is expecting a personal call they may leave their phone with the school office to answer on their behalf, or seek specific permissions to use their phone at other than their break times.
- Mobile phones and personally-owned devices will not be used in any way during lessons or formal school time. They should be switched off or silent at all times.
- Mobile phones and personally-owned mobile devices brought in to school are the responsibility of the device owner. The school accepts no responsibility for the loss, theft or damage of personally-owned mobile phones or mobile devices.
- Mobile phones and personally-owned devices are not permitted to be used in certain areas within the school site, e.g. changing rooms and toilets.
- Mobile phones will not be used during lessons or formal school time unless as part of an approved and directed curriculum-based activity with consent from a member of staff.

Students' use of personal devices

- 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, but the School strongly advises that student mobile phones should not be brought into school. The School advises that this is restricted until Years Five and Six due to children being allowed to walk home.
- If a student breaches the school policy then the phone or device will be confiscated and will be held in a secure place in the school office. Mobile phones and devices will be released to parents or carers in accordance with the school procedure.
- 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.

Staff use of personal devices

- Where staff members are required to use a mobile phone for school duties, for instance in case of emergency during off-site activities, or for contacting students or parents, then they should use their own device and hide by inputting 141 in their own mobile number for confidentiality purposes.

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.
- The school blocks/filter 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 programme 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.
- Staff are not permitted to use personal digital equipment, such as mobile phones and cameras, to record images of pupils, this includes when on field trips. However, with the express permission of the Headteacher, images can be taken provided they are transferred immediately and solely to the school's network and deleted from the staff device
- Pupils are not permitted to use personal digital equipment, including mobile phones and cameras, to record images of the others, this includes when on field trips. However with the express permission of the Headteacher, images can be taken provided they are transferred immediately and solely to the school's network and deleted from the pupil's device

Managing the IT and computing infrastructure

Internet access, security, virus protection and filtering:

This school:

- Has the educational filtered secure broadband connectivity through EXA Education.
- Uses the Surf Protect Fusion 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 is logged and only available to staff with the approved 'web filtering management' status.
- Uses USO user-level filtering where relevant, thereby closing down or opening up options appropriate to the age, stage of the students.
- Ensures network healthy through use of Sophos anti-virus software from IT Support Provider etc. and network set-up so staff and pupils cannot download executable files.
- Uses DfE, LA approved systems such as S2S, USO FX, secured email to send personal data over the Internet and uses encrypted devices or secure remote access were staff need to access personal level data off-site.
- 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 EXA Education 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 appropriate web sites. Teachers plans the curriculum context for Internet use to match pupils' ability, using child-friendly search engines where more open Internet searching is required; e.g. yahoo for kids or ask for kids , Google Safe Search and Bing.
- Be 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. Our system administrator logs or escalates as appropriate 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 programme.
- 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.
  - Uses teacher 'remote' management control tools for controlling workstations, viewing users, setting-up applications and Internet web sites, where useful.
  - 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.
  - Pupils and Staff using mobile technology, where storage of data is online, will conform to the EU data protection directive where storage is hosted within the EU.

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 schools' 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 lap tops require a password to be used.
- Requests that teachers and pupils do not switch the computers off during the day unless they are unlikely to be used again that day or have completely crashed. We request that they DO switch the computers off at the end of the day.
- Has set-up the network so that pupils cannot download executable files / programmes.
- 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 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 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 in SBM's office.
  We ensure ALL the following school stakeholders sign an Acceptable Use Agreement form. We have a system so we know who has signed.
  - staff
  - governors
  - parents

  This makes clear staffs' responsibilities with regard to data security, passwords and access.
- 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.
- We ask staff to undertaken at least annual house-keeping to review, remove and destroy any digital materials and documents which need no longer be stored.

Technical Solutions

- Staff have secure area on the network and google drive 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 os 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 school's SIRO 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 go straight to the DSLs and Online Safety Lead.
- The child/children and/or all parties involved are then 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.
- A blue form is required to be filled in and given to the DSLs, who will discuss the matter with Online Safety Coordinator if appropriate.
- To fill a blue form, collect it from in the Inclusion Room and the School Office for easy access for all staff.
- The Online Safety Coordinator 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 liase with other school)
- Parents will be referred to the website for appropriate support for future reference.
- 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.
- All incidents are logged by the Online Safety Coordinator.
- Blue forms and Incident logs are all locked in a secure cupboard.

Incident Report Forms

Blue Form:

BRIDGEWATER PRIMARY SCHOOL
CONFIDENTIAL SAFEGUARDING TRACKING/CONCERNS

Name of pupil/year:	
Concern raised by:	
Siblings in school:	
Date/Time	
Concern:	
Action/ Outcome	
Review	

Please ensure that the concern is dated, time given and that it is signed by the person raising the concern and the Designated Senior Leaders for Child Protection: Alison Harvey (HT), Frances Troop (DHT). If neither is available in school please see either Samantha Mawer, Zoe Hall or Laura White. Any additional notes or evidence should be attached securely to this form. Please note any phone numbers or contact details clearly. This form will be retained by the Designated Leaders. For recording Radicalisation concerns under the Prevent duty please use the pink form in the same way. For recording Online Safety incidents or advice regarding Online Safety please record here and notify Jenna Cox (Computing/Online Safety lead).

Incident Report Log Example:

Bridgewater Primary School Online Safety Incident Log

Date of incident	Name of individual(s) involved	Device number/location	Details of incident	Actions and reasons	Confirmed by

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

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

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 3 dedicated Online Safety lessons, alongside discussing Online Safety issues throughout the year as required. We alos 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 Jenna Cox (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

Surf Protect Filtering Information:

SurfProtect®

SurfProtect is a flexible, real-time content filtering system.

Designed from conception to place you in control, it provides you with the ability to customise the websites accessible on your internet connection and is available through three different formats:

SurfProtect Cloud is inclusive with all Exa Education connectivity services. It works by transparently intercepting the traffic and filtering it accordingly.

SurfProtect Proxy enables you to still enjoy the extensive benefits of our SurfProtect Cloud service, as well as basic HTTPS filtering, even if you are using an alternative Internet Service Provider for your connectivity.

SurfProtect Fusion works in conjunction with SurfProtect Cloud. It uses a firewall in order to implement advanced features, such as individual user filtering and reporting.

IWF Member
exa education

Which is right for me?

Essentially it depends upon the level of control you require over your filtering policy.

SurfProtect Fusion provides a greater amount of flexibiliy than is possible with SurfProtect Cloud and Proxy: by working in conjunction with a firewall, it enables filtering to a degree as specific as an individual user. It is also possible with Fusion to filter secure sites (HTTPS) - something that is of particular importance following Google's recent adoption of HTTPS across its range of services.

Alongside providing advanced filtering, Fusion also supplies user reporting. This means that as well as blocking access to banned sites, it provides information about the activity on your internet connection. From which websites are being accessed in real-time, to historical logs of all website requests, you have complete visibility.

So, if you need...

- Filtering control of HTTP websites
- Web-based portal
- Restricted social media
- Categorised filtering
- BYOD filtering
- Real-time updates
- Cost-effective solutions
- Per computer filtering
- YouTube for Education integration

SurfProtect Cloud or Proxy is perfect for you.

but if you also need...

- Customised user reporting
- Secure site (HTTPS) filtering*
- Application control (such as Skype)
- Active directory support
- Complete filtering control

*Basic HTTPS filtering is also available with SurfProtect Proxy.

SurfProtect Fusion is right for you.

How does it work?

SurfProtect's default setting automatically restricts access to the most commonly blocked web categories, so you receive instant safety from the onset. However, this can then be completely customised to create a filtering policy as strict or permissive as you would like it to be.

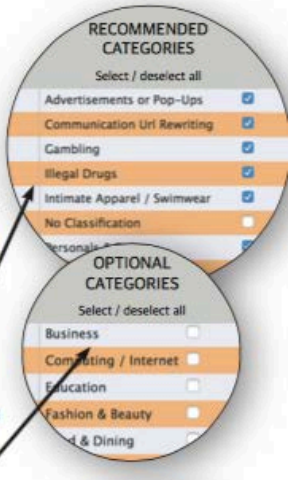
The easy-to-use, web-based portal provides you with the ability to alter the settings through its simple one-click feature:

Each website is automatically assigned to a category, access to it is then either allowed or blocked depending on the status of that category.

Divided into two groups, 'Recommended Categories' (sites which the majority of users would not want children to access) and 'Optional Categories' (sites which are subjective), the lists enable you to quicky and easily allow or block sections of the internet as appropriate.

Simply click the box alongside the category name and a tick will appear to indicate that it is now blocked. Click again and it will be allowed. The real-time update feature means that within moments your preference will be implemented.

SurfProtect's flexibiity also means that even if a website belongs to an allowed category, but you would like to block access to it, you can simply enter its address into the 'Default Blocked list' and it will update in real-time to overwrite the category's setting.



You are also able to create different profiles for different groups. There is no limit to the number of profiles you can have, and each one can have a different filtering policy. This means that you can provide staff and students with varied degrees of access, or make year group specific policies.

Did you know?

Exa is a member of the Internet Watch Foundation. The IWF was established in 1996 to provide the UK internet Hotline for child sexual abuse content to be reported in a secure and confidential way.

The IWF publishes a list of websites which contain indecent images, advertisements for, or links to such content. This list is automatically incorporated behind the scenes into SurfProtect twice daily to ensure that these websites are instantly blocked and not accessible to users.

On average, SurfProtect categorises 3500 websites a day. This means that when a user requests access to a new site that has not been seen before, it automatically assesses its content and assigns it to the appropriate category. This takes a matter of moments, enabling users to continue their web browsing without interruption.

A recent Cybersurvey conducted by Youthworks revealed that a significant number of students have been exposed to offensive or dangerous material on the internet without searching for it:

- 23% have seen sites about self-harm or suicide, with girls more likely than boys to say they have 'come across' sites like this
- 28% have come across nude pictures or videos which they did not search for
- 28% have come across very violent images they did not search for
- 20% claim to have come across websites promoting racist views
- 23% have seen websites giving advice they think could be dangerous

Questions?

If you have any questions about SurfProtect, or would like to learn more, please contact us on the details below:

0845 145 1234
education@exa.net.uk
www.exa.education
www.surfprotect.co.uk

Ofsted's E-Safety Framework and SurfProtect® Content Filtering

With Ofsted's e-safety agenda now focused upon providing students with the **knowledge** and **skills** to stay safe online, the content filtering solution employed by a school must be **flexible** and **adaptable** - rather than simply a blanket ban across all potentially inappropriate material.

That is why SurfProtect puts schools in control. Its features and flexibility combine to make a content filtering system that protects pupils, whilst also providing staff with the freedom to authorise their own e-safety decisions according to Ofsted's framework.

SurfProtect's default setting provides the building blocks to internet safety by automatically restricting access to offensive materials & categories, however these can then be altered as deemed appropriate - enabling you to create a content filtering policy as strict or permissive as you would like it to be. This can be further tailored to meet your school's needs by implementing different filtering policies for staff & students, year groups, and even individual computers. With the ability to completely customise the websites accessible on your internet connection, you are able to build an e-safety solution that works for you.

SurfProtect content filtering is inclusive with all Exa Education connectivity services.

SurfProtect content filtering is inclusive with all Exa Education connectivity services.

www.surfprotect.co.uk

exa education

The Prevent Duty

In July, the government placed a statutory duty on schools to help them keep children safe from the risk of radicalisation and extremism. This expectation made clear that every teacher must be aware of the risks posed by the online activity of extremist groups, and how social media is being used to encourage young people to travel to Syria and Iraq.

SurfProtect can be a particularly effective tool in helping schools to meet this new challenge. Here are a few ways how:

- In order to block access to radical sites, SurfProtect's default setting automatically enables the 'Intolerance & Hate' category – this prevents students viewing material online which has been identified as containing extremist content.

- The categories 'Proxy URL Rewriting' and 'Proxies/Translators' are also enabled, and therefore blocked, by default as these sites could be used by students to bypass SurfProtect and visit extremist material.

- As radical conversation and activity takes place on a variety of social media platforms – rather than designated websites – a school may also opt to restrict access to this category, and sites such as YouTube which have prolific comment sections that may be abused. SurfProtect's flexibility ensures that it is possible for a school to still allow access to the web pages, videos, or channels within these blocked categories & websites which have an educational purpose.

- We automatically include all terms identified by the DfE as being commonly used in ISIL dialogue and propaganda into the SurfProtect 'Keyword' list. This means that if a school has the 'Keyword' feature of SurfProtect activated, students will be unable to search for content including these terms. However, the customisable nature of SurfProtect ensures that each school has the ability to quickly and easily remove or add to these words, as is appropriate for their school's filtering policy.

- We continue to work tirelessly to ensure that peer to peer sites, such as Tor, are correctly categorised. This means that once a school has blocked this category, it is incredibly difficult for students to download these applications which are commonly used for sharing offensive and inflammatory content.

- It is also possible for a school to block more wide-reaching and general categories, such as News, Politics and Religion, which will include a great deal of informative material but which may also include some, or reference to, extremist content. This is a more restrictive approach, and entirely dependent upon the preference of each school as to whether it is a suitable one to adopt.

If you would like to learn more about SurfProtect, please don't hesitate to get in touch.

education@exa.net.uk | www.exa.education | 0345 145 1234