**BEWSEY LODGE PRIMARY SCHOOL**



**Online Safety Policy**

|  |  |
| --- | --- |
| Date of Review | December 2023 |
| Date of next Review | December 2024 |

# Our Safeguarding Mission Statement

Our mission is to ensure that all children and adults are safe from harm at all times and can thrive in an environment which is secure and free from abuse or bullying of any kind.

We work hard in creating a welcoming atmosphere, which develops the social and emotional needs of everyone; supporting, questioning, loving. At our school people are nurtured, valued and treated equally. Worries, concerns and thoughts are listened to and addressed in an environment of mutual respect.

At our school we are proud to feel:

**SAFE SECURE LOVED**

# Aims

In line with DfE guidance our school aims to:

* Provide a whole school approach to ensure that the teaching of online safety is firmly embedded into the curriculum and deliver an effective approach to online safety, which empowers us to protect and educate the whole school community in its use of technology
* Teach pupils about the underpinning knowledge and behaviours that can help pupils to navigate the online world safely and confidently regardless of the device, platform or app.
* Tailor our teaching and support to the specific needs of our pupils given our understanding of the risks that exist online.
* Refer to the Education for a Connected World Framework to ensure our schemes of work reflect age specific advice about the online knowledge and skills that pupils should have and the opportunity to develop at different stages of their lives.
* Have robust processes in place to ensure the online safety of pupils, staff, volunteers and governors.
* Establish clear mechanisms to identify, intervene and escalate an incident, where appropriate.

# Legislation and guidance

This policy is based on the Department for Education’s statutory safeguarding guidance, [Keeping Children Safe in Education](https://www.gov.uk/government/publications/keeping-children-safe-in-education--2), 2023 and its advice for schools on [preventing and tackling bullying](https://www.gov.uk/government/publications/preventing-and-tackling-bullying) and [searching, screening and confiscation](https://www.gov.uk/government/publications/searching-screening-and-confiscation). It also refers to the Department’s guidance on [protecting children from radicalisation](https://www.gov.uk/government/publications/protecting-children-from-radicalisation-the-prevent-duty) and [Teaching Online Safety in Schools](https://www.gov.uk/government/publications/teaching-online-safety-in-schools), DfE 2023.

It reflects existing legislation, including but not limited to the [Education Act 1996](https://www.legislation.gov.uk/ukpga/1996/56/contents) (as amended), the [Education and Inspections Act 2006](https://www.legislation.gov.uk/ukpga/2006/40/contents) and the [Equality Act 2010](https://www.legislation.gov.uk/ukpga/2010/15/contents).

In addition, it reflects the [Education Act 2011](http://www.legislation.gov.uk/ukpga/2011/21/contents/enacted), which has given teachers stronger powers to tackle cyber-bullying by, if necessary, searching for and deleting inappropriate images or files on pupils’ electronic devices where they believe there is a ‘good reason’ to do so.

The policy also takes into account the [National Curriculum computing programmes of study](https://www.gov.uk/government/publications/national-curriculum-in-england-computing-programmes-of-study) and the [Education for a Connected World](https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/759003/Education_for_a_connected_world_PDF.PDF) framework as referenced in Teaching Online Safety in Schools.

# Curriculum Context

Since September 2020, Relationships Education has been compulsory for all primary aged pupils, Relationships and Sex Education will be compulsory for all secondary aged pupils and Health Education will be compulsory in all state-funded schools in England.

Through these subjects, pupils will be taught about online safety and harms. This will include being taught what positive, healthy and respectful online relationships look like, the effects of their online actions on others and knowing how to recognise and display respectful behaviour online. Throughout these subjects, teachers will address online safety and appropriate behaviour in an age appropriate way that is relevant to their pupils’ lives.

This will complement the computing curriculum, which covers the principles of online safety at all key stages, with progression in the content to reflect the different and escalating risks that pupils face. This includes how to use technology safely, responsibly, respectfully and securely, and where to go for help and support when they have concerns about content or contact on the internet or other online technologies.

There are also other curriculum subjects which include content relevant to teaching pupils how to use the internet safely – please see appendix 11. At Bewsey Lodge our curriculum covers the breadth of topics required to ensure our pupils are receiving a fully rounded education with regard to online safety; not only how to stay safe but also how to behave online.

# Roles and Responsibilities

The Governing body has overall responsibility for monitoring this policy and holding the Headteacher, Mrs E. Williams, to account for its implementation. They will co-ordinate regular meetings with appropriate staff to discuss online safety, and monitor online safety logs as provided by the Online Safety Lead (OSL).

**The governor who oversees online safety at Bewsey Lodge Primary is Mr Nigel Spencer.**

All governors will:

* Ensure that they have read and understand this policy.
* Agree and adhere to the terms on acceptable use of the school’s ICT systems and the internet.

**The Online Safety Lead (OSL) is Mrs Gemma Nicholson** and is responsible for:

* Putting in place appropriate filtering and monitoring systems, which are updated on a regular basis and keep pupils safe from potentially harmful and inappropriate content and contact online while at school, including terrorist and extremist material.
* Ensuring that the school’s ICT systems are secure and protected against viruses and malware, and that such safety mechanisms are updated regularly.
* Conducting a full security check and monitoring the school’s ICT systems on a termly basis.
* Blocking access to potentially dangerous sites and, where possible, preventing the downloading of potentially dangerous files.
* Ensuring that any online safety incidents are logged on CPOMS and dealt with appropriately in line with this policy.
* Ensuring that any incidents of cyber-bullying are logged and dealt with appropriately in line with the school behaviour policy.
* Supporting the Headteacher in ensuring that staff understand this policy and that it is being implemented consistently throughout the school.
* Working with the Headteacher, Designated Lead for Safeguarding, Mrs L. Bailey and other staff, as necessary, to address any online safety issues or incidents.
* Updating and delivering staff training on online safety.
* Ensuring all staff have read and signed to say they have understood this policy.
* Liaising with other agencies and/or external services if necessary.
* Providing regular reports on online safety in school to the Headteacher and/or governing board.

This list is not intended to be exhaustive.

All staff, including contractors and agency staff, and volunteers are responsible for:

* Reading, signing and maintaining an understanding of this policy.
* Implementing this policy consistently.
* Agreeing and adhering to the terms on acceptable use of the school’s ICT systems and the internet (appendix 3), and ensuring that pupils follow the school’s terms on acceptable use (appendix 6).
* Working with the Designated Safeguarding Lead (DSL) and the OSL to ensure that any online safety incidents are logged on CPOMS and dealt with appropriately in line with this policy.
* Ensuring that any incidents of cyber-bullying are dealt with appropriately in line with the school behaviour policy.

This list is not intended to be exhaustive.

Parents are expected to:

* Notify Mrs G. Nicholson, Mrs L. Bailey or Mrs E. Williams of any concerns or queries regarding this policy.
* Ensure their child has read, understood and agreed to the terms on acceptable use of the school’s ICT systems and internet (appendix 6).
* Report any concerns in relation to online safety and cyber-bullying to school, to the class teacher in the first instance.

Parents can seek further guidance on keeping children safe online from the following organisations and websites:

* What are the issues? UK Safer Internet Centre: <https://www.saferinternet.org.uk/advice-centre/parents-and-carers/what-are-issues>
* Hot topics, Childnet International: <http://www.childnet.com/parents-and-carers/hot-topics>
* Parent factsheet, Childnet International: <http://www.childnet.com/ufiles/parents-factsheet-09-17.pdf>
* Internet Matters: <https://www.internetmatters.org/advice/>
* Parent Zone: <https://parentzone.org.uk/home>

Visitors and members of the community who use the school’s ICT systems or internet will be made aware of this policy, when relevant, and expected to read and follow it. If appropriate, they will be expected to agree to the terms on acceptable use (appendix 3).

# Educating Pupils about Online Safety

**Online Safety** encompasses the use of new technologies, internet and electronic communications (ICT) and also highlights the need to educate pupils about the benefits and risks of using technology and provides safeguards and awareness for users to enable them to control their online experience. It is also important to recognise the constant and fast paced evolution of ICT within our society as a whole. Therefore, it is important to focus on the underpinning knowledge and behaviours that can help pupils to navigate the online world safely and confidently regardless of the device, platform or app. This teaching is built into existing lessons across the curriculum, covered within specific online safety lessons and/or school wide approaches. Teaching is always age and developmentally appropriate.

Key knowledge and behaviours as identified by DfE are given below:

* **Evaluating what they see online** – enabling pupils to make judgements about what they see and not automatically assume that what they see is true, valid or acceptable.
* **How to recognise techniques used for persuasion** – enabling pupils to recognise the techniques that are often used to persuade or manipulate others making them less vulnerable to these techniques and better equipped to recognise and respond appropriately to strongly biased intent or malicious activity.
* **Online behaviour** – enabling pupils to understand what acceptable and unacceptable online behaviour looks like. Teaching pupils that the same standard of behaviour and honesty apply on and offline, including the importance of respect for others.
* **How to identify online risks** – enabling pupils to identify possible online risks and make informed decisions about how to act. The focus here is to help pupils assess a situation, think through the consequences of acting in different ways and decide on the best course of action.
* **How and when to seek support –** enabling pupils to understand safe ways in which to seek support if they are concerned or upset by something they have seen online.

A planned online safety programme is provided as part of ICT/Personal Health Social Economic (PHSE) and other cross curricular topics and regularly revisited – this will cover both the use of ICT and new technologies in school and outside school. Pupils will be taught in all lessons to be critically aware of the materials/content they access online and be guided to validate the accuracy of information as detailed above.

In summary, pupils will be taught about online safety as follows.

In **Key Stage 1**, pupils will be taught to:

* Use technology safely and respectfully, keeping personal information private.
* Identify where to go for help and support when they have concerns about content, contact or conduct on the internet or other online technologies.

Pupils in **Key Stage 2** will be taught to:

* Use technology safely, respectfully and responsibly.
* Recognise acceptable and unacceptable behaviour.
* Identify a range of ways to report concerns about content, contact and conduct.

The safe use of social media and the Internet will also be covered in other subjects where relevant.

The school will use assemblies to raise pupils’ awareness of the dangers that can be encountered online and may also invite speakers to talk to pupils about this.

# Educating Parents about Online Safety

The school will raise parents’ awareness of Online Safety through newsletters or other communications home, and in information via our website (See Online Safety Updates).

The NSPCC also delivers Online Safety sessions to the children in KS2. This policy will also be shared with parents on the website. If parents have any queries or concerns in relation to online safety, these should be raised in the first instance with the Online Safety Lead, Miss I. Kendal.

# Cyber-Bullying

Cyber-bullying takes place online, such as through social networking sites, messaging apps or gaming sites. Like other forms of bullying, it is the repetitive, intentional harming of one person or group by another person or group, where the relationship involves an imbalance of power (See also the school’s positive behaviour policy).

To help prevent cyber-bullying:

* We will ensure that pupils understand what it is and what to do if they become aware of it happening to them or others. We will ensure that pupils know how they can report any incidents and are encouraged to do so, including where they are a witness rather than the victim.
* The school will actively discuss cyber-bullying with pupils, explaining the reasons why it occurs, the forms it may take and what the consequences can be. Staff will discuss cyber-bullying with their class, and the issue will be addressed in assemblies.
* Teaching staff is also encouraged to find opportunities to use aspects of the curriculum to cover cyber-bullying. This includes PSHE education, and other subjects where appropriate.
* All staff, governors and volunteers (where appropriate) receive training on cyber-bullying, its impact and ways to support pupils, as part of annual safeguarding training.
* The school also sends information/leaflets on cyber-bullying to parents so that they are aware of the signs, how to report it and how they can support children who may be affected.

In relation to a specific incident of cyber-bullying, the school will follow the processes set out in the school’s positive behaviour policy. Where illegal, inappropriate or harmful material has been spread among pupils, the school will use all reasonable endeavours to ensure the incident is contained. The OSL will consider whether the incident should be reported to the police if it involves illegal material, and will work with external services if it is deemed necessary to do so.

**Acceptable Use of the Internet in School**

This policy, the ICT Policy and the Acceptable Use Policy (for all staff, governors, visitors and pupils) are inclusive of both fixed and mobile internet; technologies provided by the school (such as PCs, laptops, hand-helds, whiteboards, digital camera/video equipment, etc); and technologies owned by pupils and staff, but brought onto school premises (such as laptops, mobile phones, camera phones, PDAs and portable media players, etc).

* All pupils, parents, staff, volunteers and governors are to sign an agreement annually regarding the acceptable use of the school’s ICT systems and the internet (appendices 3 and 6). Visitors will be expected to read and agree to the school’s terms on acceptable use if relevant.
* Staff members using a work device outside school must not install any unauthorised software on the device and must not use the device in any way which would violate the school’s terms of acceptable use, as set out in appendix 3.
* Staff must ensure that their work device is secure and password-protected, and that they do not share their password with others. They must take all reasonable steps to ensure the security of their work device when using it outside school. Any USB devices containing data relating to the school must be encrypted.
* If staff has any concerns over the security of their device, they must seek advice from the DSL or OSL.
* Work devices must be used solely for work activities.

Use of the school’s Internet must be for educational purposes only, or for the purpose of fulfilling the duties of an individual’s role.  We will monitor the websites visited by pupils, staff, volunteers, governors and visitors (where relevant) to ensure they comply with the above.

## Information System Security

# School ICT systems will be managed in ways that ensure that the school meets the online safety technical requirements.

# School ICT systems will be regularly updated to ensure up-to-date anti-virus definitions and Microsoft Windows Security Updates are installed.

# There will be regular reviews and audits of the safety and security of school ICT systems.

# All users will have clearly defined access rights to school ICT systems.

# The master/administrator passwords for the school ICT system, used by the Network Manager will be available to the Headteacher or other nominated senior leader and kept in a secure place (e.g. school safe).

## E-mail

* Pupils must immediately tell a teacher if they receive offensive e-mail.
* Pupils must not reveal personal details of themselves or others in e-mail communication, or arrange to meet anyone without specific permission.

# Staff may only use approved e-mail accounts on the school system.

## Password Security

* All users read and sign an Acceptable Use Agreement to demonstrate that they have understood the Online Safety Policy.
* Pupils are not allowed to deliberately access on-line materials or files on the network, of their peers, teachers or others.
* Staff are aware of their individual responsibilities to protect the security and confidentiality of networks, SIMS and Learning Platform, including ensuring that passwords are not shared.
* Individual staff users must make sure that laptops are not left unattended and are password protected.

## Published Content and the School Website

* The contact details on the Web site should be the school address, e-mail and telephone number.
* Staff or pupils’ personal information will not be published.

## Publishing Pupils’ Images and Work

* Where possible, use general shots of classrooms or group activities rather than close up pictures of individual children. Consider the camera angle; photographs taken over the shoulder, or from behind are less identifiable.
* Images and details of pupils published together allow for the remote possibility that people outside the school could identify and then attempt to contact pupils directly. The measures described below should help to minimise the risk of such unsolicited attention.
* Use images of children in suitable dress, and take care photographing PE or swimming events to maintain modesty.
* Photographs that include pupils will be selected carefully and will have signed consent for appearance on the school website from parents.
* Pupils’ full names will not be used anywhere on the Web site, particularly in association with photographs.
* Images on website will be made more difficult to copy by publishing in low definition.
* Written permission from parents or carers will be obtained before photographs of pupils or pupils’ work are published on the school Web site. This will be done on entry to school from September 2010.

## Social Networking and Personal Publishing

* The school will block/filter access to social networking sites.
* Newsgroups will be blocked unless a specific use is approved.
* Pupils will be advised never to give out personal details of any kind which may identify them or their location.

## Managing Filtering

* The school will work with the LA, DfE and the Internet Service Provider to ensure systems to protect pupils are reviewed and improved.
* If staff or pupils discover an unsuitable site, it must be reported to the DSL or OSL.
* The OSL will ensure that regular checks are made to ensure that the filtering methods selected are appropriate, effective and reasonable.

## Managing Emerging Technologies

* Emerging technologies will be examined for educational benefit and a risk assessment will be undertaken by Headteacher and OSL before use in school is allowed.

## Mobile Phones

* Pupils are not permitted to bring mobile phones into school unless permission is sought from their class teacher.
* Unauthorised use of mobile phones will result in them being confiscated for a week.
* Staff mobile phones must be switched off/silent mode for the duration of the school day/staff meetings.
* Personal phone calls/text messaging is not permitted in the presence of pupils/other members of staff.
* All staff with a work mobile phone must read and sign an Acceptable Use Agreement to demonstrate that they have understood the Online Safety Policy (appendix 5).

## Protecting personal data

* Personal data will be recorded, processed, transferred and made available according to the Data Protection Act and GDPR 2018.
* Our School processes personal data relating to parents, pupils, staff, governors, visitors and others, and therefore is a data controller.
* The school is registered as a data controller with the ICO and will renew this registration annually.
* School has a suite of policies that meet the requirements of GDPR. These policies are located on the School website.

# Training

All new staff members will receive training, as part of their induction, on use and online safeguarding issues including cyber-bullying and the risks of online radicalisation. All staff members will receive refresher training at least once each academic year as part of safeguarding training, as well as relevant updates as required (for example through emails, e-bulletins and staff meetings).

The DSL and Deputies will undertake child protection and safeguarding training, which will include online safety, at least every 2 years. They will also update their knowledge and skills on the subject of online safety at regular intervals, and at least annually. Governors will receive training on safe Internet use and online safeguarding issues as part of their safeguarding training. Volunteers will receive appropriate training and updates, if applicable. More information about safeguarding training is set out in our child protection and CP policy.

# How the School will Respond to Issues of Misuse

Where a pupil misuses the school’s ICT systems or Internet, we will follow the procedures set out in this policy. The staff member witnessing the issue will log behaviour and safeguarding issues related to online safety. An incident report log will be made using CPOMS. The action taken will depend on the individual circumstances, nature and seriousness of the specific incident, and will be proportionate. Where a staff member misuses the school’s ICT systems or the Internet, or misuses a personal device where the action constitutes misconduct, the matter will be dealt with in accordance with the staff disciplinary procedures. The action taken will depend on the individual circumstances, nature and seriousness of the specific incident. The school will consider whether incidents, which involve illegal activity or content, or otherwise serious incidents, should be reported to the police.

# Policy Decisions

## Assessing risks

The school will take all reasonable precautions to ensure that users access only appropriate material. However, due to the international scale and linked nature of Internet content, it is not possible to guarantee that unsuitable material will never appear on a school computer. Neither the school nor Warrington LA can accept liability for the material accessed, or any consequences of Internet access. The school, in collaboration with Edac, will audit ICT provision to establish if the Online Safety policy is adequate and that its implementation is effective.

## Handling Online Safety complaints

Complaints of Internet misuse will be dealt by the DSL or OSL, and any complaints about staff misuse must be referred to the Headteacher. Complaints of a child protection nature will be dealt with in accordance with school child protection procedures and referred to Mrs L. Bailey.

***Community use of the Internet***

External organisations using the school’s ICT facilities must adhere to the Online Safety policy.

# Equal Opportunities

## Pupils with additional needs

Any pupil can be vulnerable online, and their vulnerability can fluctuate depending on their age, development stage and personal circumstances. The school endeavours to create a consistent message with parents for all pupils and this in turn should aid establishment and future development of the schools’ Online Safety rules.

However, there are some pupils, who may be more susceptible to online harm or have less support from families or friends in staying safe online. Staff are aware that some pupils may require additional teaching and support 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.

# Communicating and reviewing the Online Safety policy

## Introducing the Online Safety policy to pupils

Online Safety rules will be shared with the pupils at the start of each year and pupils will be informed that network and Internet use will be monitored.

## Staff and the Online Safety policy

All staff will be given the School Online Safety Policy and its importance explained. Staff should be aware that Internet traffic could be monitored and traced to the individual user. Discretion and professional conduct is essential.

## Enlisting parents’ support

Parents’ attention will be drawn to the Online Safety Policy in newsletters, on entry to school and on the school website. Parents/carers are asked to read through and sign acceptable use agreements on behalf of their child on admission to school. They are required to make a decision as to whether they consent to images of their child being taken/ used in the public domain (e.g. on school website).

# 

# Links with other policies

This online safety policy is linked to our:

* Child protection policy
* Positive Behaviour policy
* Staff disciplinary procedures
* Data protection policy and privacy notices
* Complaints procedure
* WBC Acceptable use of the internet policy

# Appendix 1: Online safety incident report log

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| Online Safety Incident Reporting Log | | | | | | |
| Date | Time | Incident | Action Taken | | Incident Reported By | Signature |
| What? | By Whom? |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |

# Appendix 2: Online Safety incident report form

Date: Time:

Reported by:

Person/s involved:

Type of incident:

□ bullying or harassment (cyber bullying

□ deliberately bypassing security or access

□ hacking or virus propagation

□ racist, sexist, homophobic religious hate material

□ terrorist material

□ drug/bomb making material

□ child abuse images

□ on-line gambling

□ soft core pornographic material

□ illegal hard core pornographic material

□ other (please specify)

Description of incident:

□ **Deliberate access** □ **Accidental access**

Please write here

Action taken

**Staff**

□ incident reported to head teacher/senior manager

□ advice sought from Safeguarding and Social Care

□ referral made to Safeguarding and Social Care

□ incident reported to police

□ incident reported to Internet Watch Foundation

□ incident reported to IT

□ disciplinary action to be taken

□ e-safety policy to be reviewed/amended

**Please detail any specific action taken (ie: removal of equipment)**

**□ Child/young person**

□ incident reported to head teacher/senior manager

□ advice sought from Safeguarding and Social Care

□ referral made to Safeguarding and Social Care

□ incident reported to police

□ incident reported to social networking site

□ incident reported to IT

□ child’s parents informed

□ disciplinary action to be taken

□ child/young person debriefed

□ e-safety policy to be reviewed/amended

Outcome

Signed: Date:

# Appendix 3: Acceptable use agreement (staff, governors, volunteers and visitors)

## ICT Acceptable Use Policy Agreement

ICT and the related technologies such as email, the internet and mobile devices are an expected part of our daily working life in school. This agreement 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 the Online Safety coordinator or the Head teacher.

I understand that I must use school ICT systems in a responsible way, to ensure that there is no risk to my safety or to the safety and security of the ICT systems and other users. I recognise the value of the use of ICT for enhancing learning and will ensure that students/pupils receive opportunities to gain from the use of ICT. I will, where possible, educate the young people in my care in the safe use of ICT and embed Online Safety in my work with young people.

**For my professional and personal safety:**

* The school’s information systems are school property and I understand that it is a criminal offence to use a computer for a purpose not permitted by its owner.
* I understand that the school’s information systems may not be used for private purposes, without specific permission from the Headteacher.
* I will ensure that personal data (such as data held on SIMS) 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 Headteacher or Governing Body.
* 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 to ensure policy compliance in accordance with the Data Protection Act.
* I will respect system security and I will not disclose any password or security information to anyone other than an appropriate system manager.
* I will not install any hardware of software without permission of the ICT coordinator; Technician or Headteacher.
* I will ensure that personal data is kept secure and is used appropriately, whether in school, taken off the school premises or accessed remotely.
* I will not give out my own personal details, such as mobile phone number and personal email address, to pupils.
* I will respect copyright and intellectual property rights.
* I will report any incidents of concern regarding children’s safety to the school Online Safety Coordinator or the Child Protection Coordinator.
* I will ensure that all electronic communications with pupils and staff are compatible with my professional role.
* 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 inline 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. I will ensure that when I take and/or publish images of others I will do so with their permission and in accordance with the school’s policy on the use of digital/video images.
* I will promote Online Safety with students in my care and will help them to develop a responsible attitude to system use and to the content they access or create.
* The school may exercise its right to monitor the use of the school’s information systems, including Internet access, and will delete of inappropriate materials where it believes unauthorised use of the school’s information system may be taking place, or the system may be being used for criminal purposes or for storing unauthorised or unlawful text, imagery or sound.
* I will not use chat and social networking sites in school in accordance with the school’s policies.
* I will only communicate with students/pupils and parents/carers using official school systems. Any such communication will be professional in tone and manner.
* I will not engage in any online activity that may compromise my professional responsibilities.
* When I use my personal mobile phone in school, I will follow the rules set out in the Online Safety Policy, in the same way as if I was using school equipment.
* I will ensure that any peripheral devices are protected by up to date anti-virus software and are free from viruses.
* I will not open any attachments to emails, unless the source is known and trusted, due to the risk of the attachment containing viruses or other harmful programmes.
* I will ensure that my data is regularly backed up.
* I will not install or attempt to install programmes of any type on a machine, or store programmes on a computer, nor will I try to alter computer settings.
* I will not disable or cause any damage to school equipment, or the equipment belonging to others.
* I understand that data protection policy requires that any staff or student/pupil data to which I have access will be kept private and confidential, except when it is deemed necessary that I am required by law or by school policy to disclose such information to an appropriate authority.
* I will immediately report any damage or faults involving equipment or software, however this may have happened.
* Where work is protected by copyright, I will not download or distribute copies (including music and videos).
* I understand that this Acceptable Use Policy applies not only to my work and use of school ICT equipment in school, but also applies to my use of school ICT systems and equipment out of school and my use of personal equipment in school or in situations related to my employment by the school.
* I understand that if I fail to comply with this Acceptable Use Policy Agreement, I could be subject to disciplinary action.
* I have read and understand the above and agree to use the school ICT systems (both in and out of school) and my own devices (in school and when carrying out communications related to the school) within these guidelines.

**Name:**

**Signed:**

**Date:**

# Appendix 4: Staff IT Devices - Acceptable Use Agreement

Part of Bewsey Lodge Primary’s policy is to provide portable computing devices to teachers, in order to assist in the delivery of the National Curriculum. Therefore a laptop/MacBook/iPad will be loaned to you while you remain employed at this school. While the devices are in your care the following items should be noted:

* The device remains the property of Bewsey Lodge Primary School and is only for the use of the member of staff it is issued to. Family members are not permitted to use the laptop.
* The device may **not** be used for activities unrelated to the teaching and learning at Bewsey Lodge.
* All activities related to the teaching and learning at Bewsey Lodge Primary School must be completed on school devices. Personal; laptops and home computers must not be used.
* Social networking sites (e.g. Facebook) may not be accessed from loaned devices or another other form of ICT equipment owned by the school.
* Insurance cover provides protection from the standard risks but excludes accidental damage and theft from an un-attended car. If the device is stolen from an un-attended car, you will be responsible for its replacement.
* Only software licensed by the school, authorised by the ICT Coordinator and installed by the school’s ICT staff may be used.
* Should any faults occur, the ICT Coordinator must be advised as soon as possible so that they may undertake any necessary repairs. Under no circumstances should staff attempt to fix suspected hardware faults.
* **LEA and school policies regarding appropriate use, data protection, computer misuse and health and safety must be adhered to by all users.**

|  |  |
| --- | --- |
| **Make:** |  |
| **Model:** |  |
| **Serial Number:** |  |
|  |  |
| **iPad Serial Number:** |  |

Member of Staff..............................................................................

# Appendix 5: Mobile Phone - Acceptable Use Agreement

Part of LA policy is to provide mobile phones to designated employees. While the devices are in your care the following items should be noted:

* The device remains the property of Bewsey Lodge Primary School and is only for the use of the member of staff it is issued to. Family members are not permitted to use the phone.
* The device may **not** be used for activities unrelated to Bewsey Lodge.
* Social networking sites (e.g. Facebook) may not be accessed from devices.
* **LEA and school policies regarding appropriate use, data protection, misuse and health and safety must be adhered to by all users.**

|  |  |
| --- | --- |
| **Make:** |  |
| **Model:** |  |
| **Serial Number:** |  |

Member of Staff................................................................

Signature……………………………………………………..

# Appendix 6: Acceptable use agreement (pupils and parents/carers)

## ICT Acceptable Use Agreement,

## Code of conduct: Pupils

All pupils use computer facilities including Internet access as an essential part of learning, as required by the National Curriculum. Both pupils and their parents/carers are asked to sign below to show that the Online Safety Rules have been understood and agreed.

|  |  |
| --- | --- |
| **Pupil Name:** | |
| **Pupil’s Agreement**   * I have read and I understand the school Online Safety Rules. * I will use the computer, network, mobile phones, Internet access and other new technologies in a responsible way at all times. * I know that network and Internet access may be monitored. | |
| **Signed:** | **Date:** |

|  |  |
| --- | --- |
| **Parent’s Consent for Internet Access**  I have read and understood the school Online Safety rules and give permission for my son / daughter to access the Internet. I understand that the school will take all reasonable precautions to ensure that pupils cannot access inappropriate materials but I appreciate that this is a difficult task.    I understand that the school cannot be held responsible for the content of materials accessed through the Internet. I agree that the school is not liable for any damages arising from use of the Internet facilities. | |
| **Signed:** | **Date:** |

|  |  |
| --- | --- |
| **Parent’s Consent for Web Publication of Work and Photographs**  I agree that my son/daughter’s work may be electronically published. I also agree that appropriate images and video that include my son/daughter may be published subject to the school rule that photographs will not be accompanied by complete pupil names. | |
| **Signed:** | **Date:** |
| **Please print name:** | |

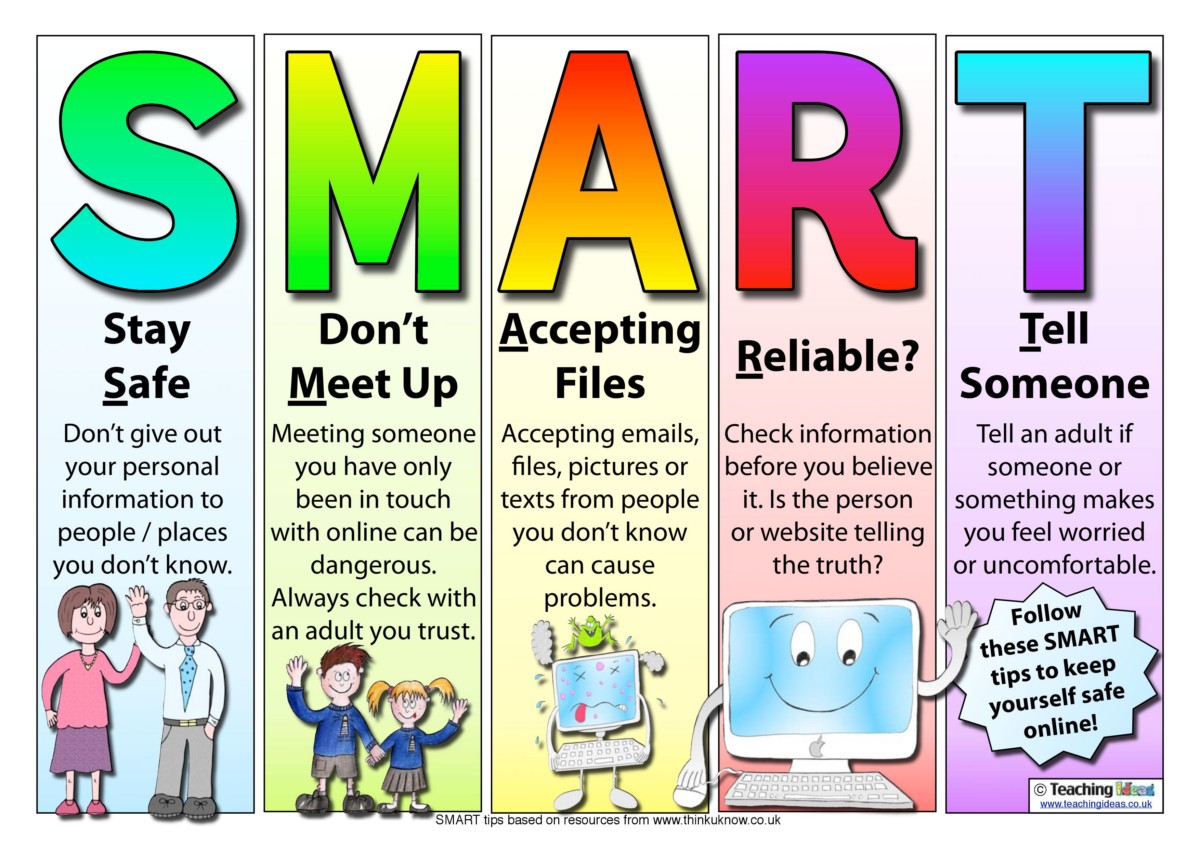
# Appendix 7 - Foundation Stage and Key Stage 1 Rules

|  |  |  |
| --- | --- | --- |
| **Think then Click** | | |
| **These rules help us to stay safe on the Internet** | | |
| We only use the internet when an adult is with us. | **We only use the internet when an adult is with us.** |  |
|  | We only use the internet when an adult is with us.  **We can click on the buttons or links when we know what they do.** |  |
| We only use the internet when an adult is with us. | **We can search the Internet with an adult.** |  |
|  | We only use the internet when an adult is with us.**We always ask if we get lost on the Internet.** |  |
| We only use the internet when an adult is with us. | **We can send and open emails together.**  We only use the internet when an adult is with us. |  |
|  | **We can write polite and friendly emails to people that we know.** |  |

# Appendix 8 - Key Stage 2 Rules

|  |
| --- |
| **Think then Click** |
| Online Safety Rules for Key Stage 2 |
| * We ask permission before using the Internet. * We only use websites that an adult has chosen. * We tell an adult if we see anything we are uncomfortable with. * We immediately close any webpage we not sure about. * We only e-mail people an adult has approved. * We send e-mails that are polite and friendly. * We never give out personal information or passwords. * We never arrange to meet anyone we don’t know. * We do not open e-mails sent by anyone we don’t know. * We do not use Internet chat rooms. |

# Appendix 9 – Online Safety Poster for classrooms



# Appendix10 Rules for Online Safety at home

|  |
| --- |
| 1. I will not give out personal information such as my address, telephone number, parents’ work address/telephone number, or the name and location of my school without my parents’ permission. |
| 1. I will tell my parents right away if I come across any information that makes me feel uncomfortable. |
| 1. I will never agree to get together with someone I ‘meet’ online without first checking with my parents. If my parents agree to the meeting, I will be sure that it is in a public place and bring my mother or father along. |
| 1. I will never send a person my picture or anything else without first checking with my parents. |
| 1. I will not respond to any messages that are mean or in any way make me feel uncomfortable. It is not my fault if I get a message like that. If I do I will tell my parents right away so that they can contact the service provider. |
| 1. I will talk with my parents so that we can set up rules for going online. We will decide upon the time of day that I can be online, the length of time I can be online and appropriate areas for me to visit. I will not access other areas or break these rules without their permission. |
| 1. I will not give out my Internet password to anyone (even my best friends) other than my parents. |
| 1. I will check with my parents before downloading or installing software or doing anything that could possibly hurt our computer or jeopardise my family’s privacy. |
| 1. I will be a good online citizen and not do anything that hurts other people or is against the law. |
| 1. I will help my parents understand how to have fun and learn things online and teach them things about the Internet, computers and other technology. |

# Appendix 11 – DfE Tables – Cross Curricular Links

The DfE document Teaching Online Safety includes a series of tables that make the cross curricular links to the key elements of online safety.

The table relating to ‘Harms and Risks’ is provided in its entirety below.

Additional tables are provided in the document for:

* Personal Safety online (Pages 15 – 20)
* Wellbeing online (Pages 20 - 23)

The full document can be accessed by double clicking the icon below when viewing this policy electronically



## Potential Harm & Risks

There are activities which although not in and of themselves harmful, could, if not understood be a risk to a child’s safety or in some cases their privacy or personal data.

| **The Potential Harm or Risk** | **Description** | **Curriculum area this could be covered in** |
| --- | --- | --- |
| Age restrictions | Some online activities have age restrictions because they include content which is not appropriate for children under a specific age.  Teaching could include:   * that age verification exists and why some sites require a user to verify their age. For example, online gambling and purchasing of certain age restricted materials such as alcohol, * why age restrictions exist - for example, they provide a warning that the site may contain disturbing material that is unsuitable for younger viewers, * helping pupils understand how this content can be damaging to under-age consumers, * the age of digital consent- the minimum age (13) at which young people can agree to share information and sign up to social media without parental consent under General Data Protection Regulations. Why it is important and what it means in practice. | **Health Education** core content – internet safety and harms. “why social media, some computer games and online gaming, for example, are age restricted”  **Computing curriculum** – some schools may want to discuss age restrictions as part of e-safety (all ages) “use technology safely and respectfully” |
| Content: How it can be used and shared | Knowing what happens to information, comments or images that are put online.  Teaching could include:   * what a digital footprint is, how it develops and how it can affect future prospects such as university and job applications, * how cookies work, * how content can be shared, tagged and traced, * how difficult it is to remove something a user wishes they had not shared, * ensuring pupils understand what is illegal online, especially what may in some cases be seen as “normal” behaviours, for example youth-produced sexual imagery (sexting). This could include copyright, sharing illegal content such as extreme pornography or terrorist content as well as the illegality of possession, creating or sharing any explicit images of a child even if created by a child. | **Relationships education** core content (all stages) – online relationships. “how information and data are shared and used online”  **Relationships education, relationships and sex education and health education** – the law “Pupils should be made aware of the relevant legal provisions when relevant topics are being taught”  **Health education** core content (all stages) – internet safety and harms “how to be a discerning consumer of information online including understanding that information, including that from search engines, is ranked, selected and targeted.”  **Computing curriculum** (all key stages) – “identify where to go for help and support when they have concerns about content or contact on the internet or other online technologies.”  **Computing curriculum** – may use this as part of wider teachings around how information online is stored and used. “protecting their online identity and privacy” |
| Disinformation, misinformation and hoaxes | Some information shared online is accidentally or intentionally wrong, misleading, or exaggerated.  Teaching could include:   * disinformation and why individuals or groups choose to share false information in order to deliberately deceive, * misinformation and being aware that false and misleading information can be shared inadvertently, * online hoaxes, which can be deliberately and inadvertently spread for a variety of reasons, * explaining that the viral nature of this sort of content can often appear to be a stamp of authenticity and therefore why it is important to evaluate what is seen online, * how to measure and check authenticity online, * the potential consequences of sharing information that may not be true. | **Relationships education** (all stages) and health education (all stages) – the law “Pupils should be made aware of the relevant legal provisions when relevant topics are being taught”  **Computing curriculum** (key stages 2 and above) - “use search technologies effectively, appreciate how results are selected and ranked, and be discerning in evaluating digital content” |
| Fake websites and scam emails | Fake websites and scam emails are used to extort data, money, images and other things that can either be used by the scammer to harm the person targeted or sold on for financial, or other gain.  Teaching could include:   * how to look out for fake URLs and websites, * ensuring pupils understand what secure markings on websites are and how to assess the sources of emails, * explaining the risks of entering information to a website which isn’t secure, * what to do if harmed/targeted/groomed as a result of interacting with a fake website or scam email. Who to go to and the range of support that is available. | **Relationships education (all stages)and health education (all stages)** – the law “Pupils should be made aware of the relevant legal provisions when relevant topics are being taught”  **Computing curriculum** (all keystages) - “use search technologies effectively, appreciate how results are selected and ranked, and be discerning in evaluating digital content” |
| Fraud (online) | Fraud can take place online and can have serious consequences for individuals and organisations.  Teaching could include:   * what identity fraud, scams and phishing are, * that children are sometimes targeted to access adults data, for example, passing on their parents or carers details (bank details, date of birth, national insurance number etc). Therefore there is a need to keep everyone’s information secure not just their own, * what “good” companies will and won’t do when it comes to personal details, for example a bank will never ask you to share a password or move money into a new account. | **Relationships education** core content – online relationships. “that people sometimes behave differently online, including by pretending to be someone they are not.”  **Computing curriculum** (all key stage) – “use search technologies effectively, appreciate how results are selected and ranked, and be discerning in evaluating digital content” |
| Password phishing | Password phishing is the process by which people try to find out your passwords so they can access protected content.  Teaching could include:   * why passwords are important, how to keep them * safe and that others may try to trick you to reveal them, * explaining how to recognise phishing scams, for example those that seek to gather login in credentials and passwords, * importance of online security to protect against viruses (such as keylogging) that are designed to access/steal/copy passwords information, * what to do when a password is compromised or thought to be compromised. | **Relationships education** core content (all stages) - online relationships. “the rules and principles for keeping safe online”  **Computing curriculum** (all key stages) – “use technology safely, respectfully and responsibly” |
| Personal data | Online platforms and search engines gather personal data. This is often referred to as ‘harvesting’ or ‘farming’.  Teaching could include:   * how cookies work, * how data is farmed from sources which look neutral, for example websites that look like games or surveys that can gather lots of data about individuals, * how, and why, personal data is shared by online companies. For example data being resold for targeted marketing by email/text (spam), * how pupils can protect themselves, including what to do if something goes wrong (for example data being hacked) and that acting quickly is essential, * the rights children have with regard to their data, including particular protections for children under the General Data Protection Regulations (GDPR), how to limit the data companies can gather including paying particular attention to boxes they tick when playing a game or accessing an app for the first time | **Relationships education** core content (all stages) – online relationships. “how information and data is shared and used online”  **Computing curriculum** (all key stages) – “use technology purposefully to create, organise, store, manipulate and retrieve digital content.  **Computing curriculum** (all key stages) – “use technology safely and respectfully, keeping personal information private” |
| Persuasive design | Many devices/apps/games are designed to keep users online for longer than they might have planned or desired.  Teaching could include:   * explaining that the majority of games and platforms are businesses designed to make money. Their primary driver is to encourage users to be online for as long as possible to encourage them to spend money (sometimes by offering incentives and offers) or generate advertising revenue, * how designers use notification to pull users back online. | **Health education** core content (all stages) – internet safety and harms. “about the benefits of rationing time spent online, the risks of excessive internet time spent on electronic devices and the impact of positive and negative content online on their own and others’ mental and physical wellbeing”  **Computing curriculum** (all key stages) – “use technology safely, respectfully and responsibly” |
| Privacy settings | Almost all devices, websites, apps and other online services come with privacy setting that can be used to control what is shared.  Teaching could include:   * how to find information about privacy setting on various sites, apps, devices and platforms, * explaining that privacy settings have limitations, for example they will not prevent someone posting something inappropriate. | **Relationships education** core content – online relationships. “the rules and principles for keeping safe online, how to recognise risks, harmful content and contact, and how to report them.”  **Computing curriculum** (all key stages) – “understand a range of ways to use technology safely, respectfully, responsibly and securely, including protecting their online identity and privacy” |
| Targeting of online content  Including on social media and search engines. | Much of the information seen online is a result of some form of targeting.  Teaching could include:   * how adverts seen at the top of online searches and social media feeds have often come from companies paying to be on there and different people will see different adverts, * how the targeting is done, for example software which monitors online behaviour (sites they have visited in the past, people who they are friends with etc) to target adverts thought to be relevant to the individual user, * the concept of clickbait and how companies can use it to draw people onto their sites and services. | **Health education** – core content (all stages) - internet safety and harms. “how to be a discerning consumer of information online including understanding that  information, including that from search engines, is ranked, selected and targeted”  **Computing curriculum** (all key stages) – “use search technologies effectively, appreciate how results are selected and ranked, and be discerning in evaluating digital content” |

## How to Stay Safe Online

This section of the guidance covers elements of online activity that could adversely affect a pupil’s personal safety or the personal safety of others online (pages 15-20).

Age specific advice on these can be found in the following sections of the Education for a Connected World framework

* Online relationships
* Privacy and Security
* Online reputation
* Online bullying

## Wellbeing

This section of the guidance covers the elements of online activity that can adversely affect a pupil’s wellbeing (Pages 20-23).

* Age specific advice on these can be found in the following sections of the Education for a Connected World framework: Self-image and identity
* Online reputation
* Online bullying
* Health, wellbeing and lifestyle