GISBURN ROAD C.P. SCHOOL BARNOLDSWICK

ONLINE SAFETY POLICY

DATE AGREED: MARCH 2024

REVIEW DATE: MARCH 2026

Gisburn Road Primary School Online Safety Policy

Aims

Our school aims to:

- Have robust processes in place to ensure the online safety of pupils, staff, volunteers and governors
- Deliver an effective approach to online safety, which empowers us to protect and educate the whole school community in its use of technology
- 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, and its advice for schools on preventing and tackling bullying and searching, screening and confiscation. It also refers to the Department's guidance on protecting children from radicalisation. It reflects existing legislation, including but not limited to the Education Act 1996 (as amended), the Education and Inspections Act 2006 and the Equality Act 2010. In addition, it reflects the Education Act 2011, 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.

Roles and responsibilities

The governing body - The governing body has overall responsibility for monitoring this policy and holding the headteacher to account for its implementation. The governing body will co-ordinate regular meetings with appropriate staff to discuss online safety, and monitor online safety logs as provided by the designated safeguarding lead (DSL).

The governor who oversees online safety is Mrs Waddington. Mrs Waddington will report regularly to the governing body.

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 (appendix 2)
-

The headteacher - The headteacher is responsible for ensuring that staff understand this policy, and that it is being implemented consistently throughout the school.

The designated safeguarding lead - Details of the school's designated safeguarding lead (DSL) are set out in our Safeguarding and Child Protection Policy.

The DSL takes lead responsibility for online safety in school, in particular:

- Ensuring that staff understand this policy and that it is being implemented consistently throughout the school
- Working with ICT Lead, Schools ICT support and other staff, as necessary, to address any online safety issues or incidents
- Ensuring that any online safety incidents are logged (see appendix 5) 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
- Updating and delivering staff training on online safety (appendix 4 contains a self-audit for staff on online safety training needs)
- Liaising with other agencies and/or external services if necessary
- Providing regular reports on online safety in school to the headteacher and/or governing body

The ICT Lead - The ICT lead 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. (Alongside Primary Technology)
- Ensuring that any online safety incidents are logged (see appendix 5) and dealt with appropriately in line with this policy
- Monitoring the filtering system and producing regular reports. (Alongside Primary Technology)

School ICT support-Primary Technology

- The ICT support is responsible for:
- 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 regular basis
- Blocking access to potentially dangerous sites and, where possible, preventing the downloading of potentially dangerous files

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

- 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 2/3), and ensuring that pupils follow the school's terms on acceptable use (appendix 1)
- Working with the DSL to ensure that any online safety incidents are logged (see appendix 5) 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

Parents - Parents are expected to:

- Notify a member of staff or the headteacher 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 1)

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/advicecentre/parentsand-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

Visitors and members of the community 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 2). Visitors will also be informed about the use of mobile phones in school through the visitor information sheet in the entrance hall.

Online filtering and monitoring systems

Gisburn Road uses **Netsweeper** website **filtering**. It is updated on a regular basis and keeps pupils safe from potentially harmful and inappropriate content and contact online while at school, including terrorist and extremist material. Netsweeper confirmed that their service fully meets the issues identified in a specific checklist by UK Safer Internet Centre (Date of assessment June 2018).
https://www.saferinternet.org.uk/advice-centre/teachers-and-school-staff/appropriate-filtering-and-monitoring

Online Safety Cluster Group In school we have an online safety cluster group which involves the headteacher, Computing Lead, and the online safety governor. We meet every half term to discuss and act upon relevant online safety issues to ensure it holds a high priority within school.

Educating pupils about online safety Pupils will be taught about online safety as part of the curriculum.

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 or contact 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 and contact
- Online safety is taught regularly as a discrete lesson, sometimes as part of the PSHE curriculum. Discrete lessons occur at least once per half term alongside regular updates and teaching points as and when they arise. EYFS and KS1 children are taught online safety using the SWGFL scheme. https://www.gov.uk/government/publications/education-for-a-connected-world

A progression grid is currently developing with this new scheme to monitor progression and coverage.

Educating parents about online safety The school will raise parents' awareness of internet safety in letters or other communications home, and in information via our website. This policy will also be shared with parents. In addition we hold online safety days in school. Parents are invited to participate in these sessions. If parents have any queries or concerns in relation to online safety, these should be raised in the first instance with the headteacher and/or the DSL. Concerns or queries about this policy can be raised with any member of staff or the headteacher.

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. 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. Class teachers will discuss cyber-bullying with their class and the issue will be addressed in assemblies.

Teaching staff are also encouraged to find opportunities to use aspects of the curriculum to cover cyber-bullying. This includes personal, social, health and economic (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 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 anti-bullying 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 DSL 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.

Boost tools SWGFL

Whisper. Pupils and parents can use Whisper on the school website for reporting cyber-bullying concerns to school. Pupils and parents can do this anonymously if they choose. Whisper posters are placed in all children's toilets and around school.

Reputation Alerts. Reputation Alerts is a tool that enables you to enter search keywords and phrases, which will then monitor the World Wide Web for content that matches. This is very useful for seeing who and what is being talked about regarding Gisburn Road Primary or staff on the Internet.

Sexting In cases where this is reported to school we will follow the UK Council for Internet Safety Guidance 'Sexting in Schools and Colleges'.

Examining electronic devices

School staff have the specific power under the Education and Inspections Act 2006 (which has been increased by the Education Act 2011) to search for and, if necessary, delete inappropriate images or files on pupils' electronic devices, including mobile phones, iPads and other tablet devices, where they believe there is a 'good reason' to do so. When deciding whether there is a good reason to examine or erase data or files on an electronic device, staff must reasonably suspect that the data or file in question has been, or could be, used to:

- Cause harm, and/or
- Disrupt teaching, and/or
- Break any of the school rules

If inappropriate material is found on the device, it is up to the staff member in conjunction with the DSL or other member of the senior leadership team to decide whether they should:

- Delete that material, or
- Retain it as evidence (of a criminal offence or a breach of school discipline), and/or
- Report it to the police

Any searching of pupils will be carried out in line with the DfE's latest guidance on screening, searching and confiscation.

Any complaints about searching for or deleting inappropriate images or files on pupils' electronic devices will be dealt with through the school complaints procedure.

Acceptable use of the internet in school

Pupils, parents, staff, volunteers and governors are expected to sign an agreement regarding the acceptable use of the school's ICT systems and the internet (appendices 1 and 2). The following outlines this further.

- All devices with 3G/4G wireless connections can access unfiltered internet content. Therefore, this facility must be turned off before children use such devices.
- All children, on induction to the school, are required to consent to the use of photographs, videos and appearance in local (or national) media. An up-to-date list of permissions is kept in the school office, where staff can access them prior to taking any pictures and videos. A child's parents/carers can change these permissions at any time by notifying the school office, where a new form will need to be completed and signed.
- Full names or personal details will not be used on any digital media that is published.
- Parents/Carers are permitted to video or photograph certain school events, such as school productions and assemblies. Parents will be reminded not to share images on social media or video sharing sites. Events may be recorded by the school, or by a private company assigned by the school, and later made available for parents/carers to purchase. Parents/Carers who do not wish their child to be photographed/recorded can express these wishes to the Head teacher or other staff, who will make appropriate arrangements.
- Staff are trained to understand the risks associated with publishing images and the school policy of not publishing an image where it can be linked to the name of a child.
- Photographs/videos should only be taken using school equipment, for school purposes. This content should only be stored on equipment that is for predominantly school use. Staff should always make sure that children are appropriately dressed and not participating in activities that could be misinterpreted.
- All staff, parents/carers, and pupils are made aware of the dangers of publishing images and videos of pupils or adults on Social Network sites without the consent of the persons involved. - See the school's Social Media Policy.

- The guidelines for safe practice and relevant Acceptable Use Policies are monitored every year by the Digital Safety champion, who will liaise with the Headteacher as required.

Visitors will be expected to read and agree to the school's terms on acceptable use if relevant. 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. More information is set out in the acceptable use agreements in appendices 1 and 2.

Pupils using mobile devices in school
Mobile phones for children are not permitted in school. All mobile phones brought into school by pupils are held in the school office until the end of the school day. Any breach of the acceptable use agreement by a pupil may trigger disciplinary action in line with the school behaviour policy, which may result in the confiscation of their device.

Staff using mobile phones in school
Staff mobile phones should be stored securely in bags or cupboards, not kept out on desks/surfaces in the classroom. Staff are not permitted to make or take phone calls on their mobile phones in lesson time. Phone calls can be taken/made in breaks/lunchtime but a quiet, private area away from children or other staff must be used. Staff are NOT permitted to take any images of pupils/school on their mobile phones.

Social Media
The use of social media networks by staff is covered in the school Social Media Policy.

Visitors using mobile phones in school
Visitors to school are not permitted to use their mobile phones to make or take calls within the school building. They must leave the premises to do this. This information will be shared with visitors through the 'Visitor Information Sheet' at the School Office Desk. Parent visitors attending Celebration Assemblies may take photographs of their child, but these must be of their child only and must only before personal use (i.e. not shared on social media). Visitors will be politely asked to lock their belongings including their phones in a locker.

Staff using work devices outside school
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 cannot be used due to threat of loss. (GDPR regulations) If staff have any concerns over the security of any their device, they must seek advice from the ICT Lead. Work devices must be used solely for work activities. During school trips, staff will be required to carry mobile phones. Contact details will be left with the base contact for emergency purposes.

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 the behaviour policy. 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.

Training
All new staff members will receive training, as part of their induction, on safe internet 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 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. Separate training sessions focused on online safety are also delivered to governors. Volunteers will receive appropriate training and updates, if applicable.

Dealing with incidents
In the event that a Digital Safety incident occurs, that contravenes the Digital Safety Policy or agreed Acceptable Use Policy, it is important the protocol below will be followed. It is important to distinguish between illegal and inappropriate use of ICT. All incidents will be logged in the incident log.

Illegal offences
Any suspected illegal material or activity must be brought to the immediate attention of the Head teacher who must refer this to external authorities, e.g. Police, CEOP, Internet Watch Foundation (IWF).

The school will never personally investigate, interfere with or share evidence as this may inadvertently be committing an illegal offence.

The school will always report potential illegal content to the Internet Watch Foundation (http://www.iwf.org.uk) as they are licensed to investigate – schools are not.
Examples of illegal offences are:

- Accessing child sexual abuse images
- Accessing non-photographic child sexual abuse images
- Accessing criminally obscene adult content
- Incitement to racial hatred

More details regarding these categories can be found on the IWF website - http://www.iwf.org.uk.

eSafety across the curriculum
Digital Safety is embedded in all areas of the computing curriculum. Other issues such as Cyber-bullying and 'Grooming' are discussed in PSHE sessions. Where necessary, class teachers will differentiate their teaching to ensure all pupils remain safe when using technology.
Digital Safety rules are displayed wherever computers are used in school. This is differentiated by key stage.

Digital Safety – Raising staff awareness
All staff, upon starting work at the school, are required to agree to the school's Acceptable Use Policy and are provided with a copy of the Digital Safety policy. Staff training updates for Digital Safety will be delivered as necessary, with a minimum of once per academic year. All training and advice will be delivered by the Computing Subject Leader. The Computing Subject Leader/ Digital Safety Champion is aware of updates to Digital Safety guidelines and receives external training as necessary.

All staff are expected to promote and model responsible use of ICT at all times, and all staff are responsible for promoting Digital Safety whilst using ICT.

Digital Safety – Raising parents/carers awareness

"Parents often either underestimate or do not realise how often children and young people come across potentially harmful and inappropriate material on the internet and are often unsure about what they would do about it." (Byron Report, 2008).

Gisburn Road offers regular opportunities for parents/carers and the wider community to be informed about Digital Safety, including the benefits and risks of using various technologies. This takes place through:

- School newsletters
- A dedicated area on the school website, which promotes external Digital Safety resources and online materials
- Parents Digital Safety Awareness sessions and advice available from the Digital Safety champion

Monitoring arrangements

Staff will use CPOMS to add behaviour and safeguarding issues related to online safety. An incident report log can be found in appendix 5 for the ICT Lead.

This policy will be reviewed annually by the Online Safety Group. At every review, the policy will be shared with the governing body.

Links with other policies

This online safety policy is linked to our:

- Child protection and safeguarding policy
- Behaviour policy
- Staff disciplinary procedures
- Data protection policy and privacy notices
- Complaints procedure

Appendix 1: Acceptable use agreement (Pupils)

Gisburn Road

Community Primary School

Together we… dream it… believe it… achieve it!

Pupil Acceptable Use Policy Agreement (Foundation / KS1)

This is how we stay safe when we use computers:

- I will ask a teacher if I want to use the computers.
- I will only use activities that a teacher has allowed me to use.
- I will take care of the computer and other equipment.
- I will ask for help from a teacher if I am not sure what to do or if I think I have done something wrong.
- I will tell a teacher if I see something that upsets me on the screen.
- I know that if I break the rules I might not be allowed to use a computer.

Name of Child: …… Signed (Child):……

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

I know that my son / daughter has signed an Acceptable Use Agreement and has received, or will receive, e-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 Policy.

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 e-safety.

Signed: _____ Date: _____

With signing this document you're agreeing to make yourself aware of current digital safety advice and necessary age restrictions for films, games, music and online platforms. This can be done through attending parent school digital safety sessions, accessing the schools digital safety page or any of the agencies below.

Pupil Acceptable Use Agreement (KS2)

Digital technologies have become integral to the lives of children and young people, both within schools and outside school. These technologies are powerful tools, which open up new opportunities for everyone. These technologies 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 Policy is intended to ensure:

- that young people will be responsible users and stay safe while using the internet and other digital technologies 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.

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.

Acceptable Use Policy Agreement

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.

For my own personal safety:

- I understand that the school will monitor my use of the systems, devices and digital communications.
- I will be aware of "stranger danger", when I am communicating on-line.
- I will not share personal information about myself or others when on-line (this could include names, addresses, email addresses, telephone numbers, age, gender, educational details, financial details etc)
- I will immediately report any unpleasant or inappropriate material or messages or anything that makes me feel uncomfortable when I see it on-line to a member of staff.

I will act as I expect others to act toward me:

- I will respect others' work and property and will not access, copy, remove or otherwise alter any other user's files, without the owner's knowledge and permission.
- I will be polite and responsible when I communicate with others, I will not use strong, aggressive or inappropriate language and I appreciate that others may have different opinions.
- I will not take or distribute images of anyone without their permission.

I recognise that the school has a responsibility to maintain the security of the technology

- I will only use my own personal devices in school if I have permission.
- I understand that, if I do use my own devices in school, I will follow the rules set out in this agreement, in the same way as if I was using school equipment.
- I understand the risks and will not try to upload, download or access any materials which are illegal or inappropriate or may cause harm or distress to others, nor will I try to use any programmes or software that might allow me to bypass the filtering / security systems in place to prevent access to such materials.
- I will immediately report any damage or faults involving equipment or software, however this may have happened.
- I will not open any hyperlinks in emails or any attachments to emails, unless I know and trust the person / organisation who sent the email, or if I have any concerns about the validity of the email (due to the risk of the attachment containing viruses or other harmful programmes).
- I will not install or attempt to install or store programmes of any type on any school device, nor will I try to alter computer settings.

I understand that I am responsible for my actions, both in and out of school:

I understand that the school also has the right to take action against me if I am involved in incidents of inappropriate behaviour, that are covered in this agreement, when I am out of school and where they involve my membership of the school community (examples would be cyber-bullying, use of images or personal information) and contact my parents if I am using technologies not designed for my age, for example, Facebook, Instagram, Snapchat etc.

I understand that if I fail to comply with this Acceptable Use Policy Agreement, I will be subject to disciplinary action. This may include loss of access to the school network / internet, detentions, exclusions, contact with parents and in the event of illegal activities involvement of the police.

Pupil Acceptable Use Agreement Form

This form relates to the Acceptable Use Agreement, to which it is attached.

Please complete the sections below to show that you have read, understood and agree to the rules included in the Acceptable Use Agreement. If you do not sign and return this agreement, access will not be granted to school ICT systems.

I have read and understand the above and agree to follow these guidelines when:

- I use the school systems and devices (both in and out of school).
- I use my own devices in the school (when allowed) eg mobile phones, gaming devices, USB devices, cameras etc
- I use my own equipment out of the school in a way that is related to me being a member of this academy eg communicating with other members of the school, accessing school email, VLE, website etc.

Name of Pupil: _____ Class: _____

Signed: _____ Date: _____

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

I know that my son / daughter has signed an Acceptable Use Agreement and has received, or will receive, e-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 Policy.

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 e-safety.

Signed: _____ Date: _____

With signing this document you're agreeing to make yourself aware of current digital safety advice and necessary age restrictions for films, games, music and online platforms. This can be done through attending parent school digital safety sessions, accessing the schools digital safety page or any of the agencies below.

Appendix 2: acceptable use agreement (governors, volunteers and visitors)

Acceptable use of the school's ICT systems and the internet: agreement for staff, governors, volunteers and visitors	
Name of staff member/governor/volunteer/visitor:	
When using the school's ICT systems and accessing the internet in school, or outside school on a work device, I will not: • Access, or attempt to access inappropriate material, including but not limited to material of a violent, criminal or pornographic nature • Use them in any way which could harm the school's reputation • Access social networking sites or chat rooms • Use any improper language when communicating online, including in emails or other messaging services • Install any unauthorised software • Share my password with others or log in to the school's network using someone else's details •	
I will only use the school's ICT systems and access the internet in school, or outside school on a work device, for educational purposes or for the purpose of fulfilling the duties of my role. I agree that the school will monitor the websites I visit. I will take all reasonable steps to ensure that work devices are secure and password-protected when using them outside school, and keep all data securely stored in accordance with this policy and the school's data protection policy. I will let the designated safeguarding lead (DSL) and ICT manager know if a pupil informs me they have found any material which might upset, distress or harm them or others, and will also do so if I encounter any such material. I will always use the school's ICT systems and internet responsibly, and ensure that pupils in my care do so too.	
Signed (staff member/governor/volunteer/visitor):	**Date:**

Appendix 3: Acceptable Use Policy for staff

Gisburn Road

Community Primary School

Together we… dream it… believe it… achieve it!

Access and professional use

- All computer networks and systems belong to the school and are made available to staff for educational, professional and purposes deemed appropriate by the Head Teacher and Governing Body.
- Staff are expected to abide by all school Digital Safety rules and the terms of this Acceptable Use Policy. Failure to do so may result in disciplinary action being taken.
- The school reserves the right to monitor internet activity and examine and delete files from the school's system.
- Staff have a responsibility to safeguard pupils in their use of the internet and reporting all Digital Safety concerns to the appropriate persons.
- Copyright and intellectual property rights in relation to materials used from the internet must be respected.
- Emails and other written communications must be carefully written and polite in tone and nature.
- Anonymous messages and the forwarding of chain letters are not permitted.
- Staff should only access internet sites in school that are accessible using the school's filtering system. The use of chat rooms is not permitted

Data protection and system security

- Staff should ensure that any personal data sent over the internet will be sent securely. Where personal data is taken off the school premises via laptops and other mobile systems, the information must remain secure.
- Sharing and use of other people's log on details and passwords is forbidden. Sensitive data should not be left of screens visible to parents and visitors

Personal use

- Staff should not browse, download or send material that could be considered offensive to colleagues and pupils or is illegal.
- Staff should not allow school equipment or systems to be used or accessed by unauthorised persons and keep any school computers or hardware used at home safe.
- Staff should ensure that personal websites or blogs do not contain material that compromises their professional standing or brings the school's name into disrepute.

I have read the above policy and agree to abide by its terms.

Name:

Signed:

Date:

Appendix 4: online safety training needs – self-audit for staff

Online safety training needs audit	
Name of staff member/volunteer:	**Date:**
Do you know the name of the person who has lead responsibility for online safety in school?	
Do you know what you must do if a pupil approaches you with a concern or issue?	
Are you familiar with the school's acceptable use agreement for staff, volunteers, governors and visitors?	
Are you familiar with the school's acceptable use agreement for pupils and parents?	
Do you regularly change your password for accessing the school's ICT systems?	
Are you familiar with the school's approach to tackling cyber-bullying?	
Are there any areas of online safety in which you would like training/further training? Please record them here.	

Appendix 5: online safety incident report log

Online safety incident report log				
Date	**Where the incident took place**	**Description of the incident**	**Action taken**	**Name and signature of staff member recording the incident**