Our Lady of the Wayside Catholic Primary School

Online Safety and Acceptable Use Agreement Policy

Date written	**January 2023**
Date of last update	**February 2024**
Date agreed and ratified by governing body or management committee	**19/02/2024**
Date of next full review	**Spring 2025**

Contents

1. 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

2. Legislation and guidance

This policy is based on the Department for Education's (DfE) statutory safeguarding guidance, Keeping Children Safe in Education, and its advice for schools on:

- Teaching online safety in schools
- Preventing and tackling bullying and cyber-bullying: advice for headteachers and school staff
- [Relationships and sex education
- Searching, screening and confiscation

It also refers to the DfE'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.

3. Roles and responsibilities

3.1 The governing board

The governing board has overall responsibility for monitoring this policy and holding the headteacher to account for its implementation.

The governing board 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 Mary McHale (Safeguarding Governor)

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 3)

3.2 The headteacher

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

3.3 The designated safeguarding lead

Details of the school's DSL and deputies are set out in our child protection and safeguarding policy as well as relevant job descriptions.

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

- Supporting the headteacher in ensuring that staff understand this policy and that it is being implemented consistently throughout the school
- Working with the headteacher, 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 board

This list is not intended to be exhaustive.

3.4 The ICT support team

The ICT support team are 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
- Blocking access to potentially dangerous sites and, where possible, preventing the downloading of potentially dangerous files

This list is not intended to be exhaustive.

3.5 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 3), and ensuring that pupils follow the school's terms on acceptable use (appendices 1 and 2)
- 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

This list is not intended to be exhaustive.

3.6 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 (appendices 1 and 2)

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

- What are the issues? - UK Safer Internet Centre
- Hot topics - Childnet International
- Parent factsheet - Childnet International
- Healthy relationships – Disrespect Nobody

3.7 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 3).

4. Educating pupils about online safety

Pupils will be taught about online safety as part of the curriculum:

Under the new RHE requirements, **we will teach** teach:

- Relationships education and health education in primary schools
- Relationships and sex education and health education in secondary schools

This new requirement includes aspects about online safety as set out in the new RHE documentation expectations are in italics.

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

*By the **end of primary school**, pupils will know:*

- *That people sometimes behave differently online, including by pretending to be someone they are not*

- *That the same principles apply to online relationships as to face-to-face relationships, including the importance of respect for others online including when we are anonymous*
- *The rules and principles for keeping safe online, how to recognise risks, harmful content and contact, and how to report them*
- *How to critically consider their online friendships and sources of information including awareness of the risks associated with people they have never met*
- *How information and data is shared and used online*
- *How to respond safely and appropriately to adults they may encounter (in all contexts, including online) whom they do not know*

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

<table>
<tr><th colspan="5">Overview of Online Safety lessons-This will be covered in the Autumn Term alongside the RHE curriculum</th></tr>
<tr><th></th><th>Lesson 1</th><th>Lesson 2</th><th>Lesson 3</th><th>Lesson 4</th></tr>
<tr><td rowspan="2">Year R</td><td colspan="4">Self-regulation, Managing self, Understanding the wider world</td></tr>
<tr><td colspan="4">To recognise the value of technology and use it safely
To positively use technology</td></tr>
<tr><td rowspan="3">Year 1</td><td>Using the internet safely</td><td>Online Emotions</td><td>Always be kind and considerate</td><td>Posting and sharing online</td></tr>
<tr><td>WALT: I can describe what the internet is and how to use it safely.</td><td>WALT: I can identify different feelings using the internet.</td><td>WALT: I can describe how to treat others, both online and in-person.</td><td>WALT: I can explain the importance of being careful about what we post and share online.</td></tr>
<tr><td colspan="4">NC objectives: Pupils should be taught to:
Recognise common uses of information technology beyond school
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</td></tr>
<tr><td rowspan="3">Year 2</td><td>What happens when I post online?</td><td>How do I keep my things safe online?</td><td>Who should I ask?</td><td>It's My Choice</td></tr>
<tr><td>WALT: I can explain what happens to information posted online.</td><td>WALT: I can identify how to keep things safe and private online.</td><td>WALT: I can explain what should be done before sharing information online.</td><td>WALT: I can explain why I have the right to say no and deny permission.</td></tr>
<tr><td colspan="4">NC objectives: Pupils should be taught to:
Recognise common uses of information technology beyond school
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</td></tr>
</table>

Year 3	**Beliefs, opinions and facts on the internet**	**When being online makes me upset**	**Sharing of information**	**Rules of social media platforms**
	WALT: I can explain how the internet can be used to share beliefs, opinions and facts.	WALT: I can describe the effects that some internet use can have on our feelings and emotional wellbeing.	WALT: I can identify the ways personal information can be shared on the internet.	WALT: I can describe the rules for social media platforms.
	NC objectives: Pupils should be taught to: • Use search technologies effectively, appreciate how results are selected and ranked, and be discerning in evaluating digital content. • Select, use and combine a variety of software (including internet services) on a range of digital devices to design and create a range of programs, systems and content that accomplish given goals, including collecting, analysing, evaluating and presenting data and information. • Use technology safely, respectfully and responsibly; recognise acceptable/unacceptable behaviour; identify a range of ways to report concerns about content and contact.			

	Lesson 1	**Lesson 2**	**Lesson 3**	**Lesson 4**	**Lesson 5**	**Lesson 6**
Year 4	**What happens when I search online?**	**How do companies encourage us to buy online?**	**Fact, opinion or belief?**	**What is a bot?**	**What is my #TechTimetable like?**	**How can I be safe and respectful online?**

	WALT: I know how to search for information within a wide group of technologies and judge its accuracy.	WALT: I can describe some of the methods used to encourage people to buy things online.	WALT: I can explain why lots of people sharing the same opinions or beliefs online do not make those opinions or beliefs true.	WALT: I can explain that technology can be designed to act like or impersonate living things	WALT: I can explain how technology can be a distraction and identify when I might need to limit the amount of time spent using technology.	WALT: I can understand how to be safe and respectful online.
	NC objectives: Pupils should be taught to: • Use technology safely, respectfully and responsibly; recognise acceptable/unacceptable behaviour; identify a range of ways to report concerns about content and contact.					
Year 5	**Online Protection**	**Online Communication**	**Online Reputation**	**Online Bullying**	**Online Health**	
	WALT: I can explain how apps can access our personal information and how to alter the permissions.	WALT: I can identify positive and negative aspects of online communication.	WALT: I can identify how online information can be used to form judgements.	WALT: I can identify ways to overcome online bullying.	WALT: I can describe how technology can affect health and wellbeing.	-
	NC objectives: Pupils should be taught to: • Understand computer networks including the internet; how they can provide multiple services, such as the world wide web; and the opportunities they offer for communication and collaboration • Use technology safely, respectfully and responsibly; recognise acceptable/unacceptable behaviour; identify a range of ways to report concerns about content and contact.					
Year 6	**Life Online**	**Sharing Online**	**Creating a positive online reputation**	**Capturing Evidence**	**Password Protection**	**Think before you click**
	WALT: I can describe issues online that give us negative feelings and know	WALT: I can think about the impact and consequences of	WALT: I can describe how to create a positive online	WALT: I can describe how to capture bullying content as	WALT: I can manage personal passwords effectively.	WALT: I can describe strategies to help be protected online.

	ways to get help.	sharing online.	reputation.	evidence.		
	NC objectives: Pupils should be taught to: • Use technology safely, respectfully and responsibly; recognise acceptable/unacceptable behaviour; identify a range of ways to report concerns about content and contact.					

5. Educating parents about online safety

The school will raise parents' awareness of internet safety in letters or other communications home, and in information via weekly newsletter.

This policy will also be shared with parents.

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.

6. Cyber-bullying

6.1 Definition

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.

6.2 Preventing and addressing cyber-bullying

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 tutor groups.

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 (see section 11 for more detail).

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 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 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.

6.3 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 and the school's COVID-19 risk assessment.

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

7. Acceptable use of the internet in school

All 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 1-3). 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, 2 and 3.

8. Pupils using mobile devices in school

Pupils in Year 6 may bring mobile devices into school, but are not permitted to use them during the school day. They are only used as a form of communication with their parents both before school and afterschool if they travel to school independently.

These devices will be stored in a locked box within the year 6 classroom.

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.

9. Staff using work devices outside school

All staff members will take appropriate steps to ensure their devices remain secure. This includes, but is not limited to:

- Keeping the device password-protected – strong passwords are at least 8 characters, with a combination of upper and lower-case letters, numbers and special characters (e.g. asterisk or currency symbol)
- Ensuring their hard drive is encrypted – this means if the device is lost or stolen, no one can access the files stored on the hard drive by attaching it to a new device
- Making sure the device locks if left inactive for a period of time
- Not sharing the device among family or friends
- Installing anti-virus and anti-spyware software
- Keeping operating systems up to date – always install the latest updates

Staff members must not use the device in any way which would violate the school's terms of acceptable use, as set out in appendix 3.

Work devices must be used solely for work activities.

If staff have any concerns over the security of their device, they must seek advice from the ICT support team

10. 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 our policies on behaviour and ICT and internet acceptable use. 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/staff code of conduct. 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.

11. 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 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 safeguarding policy.

12. Monitoring arrangements

The DSL logs behaviour and safeguarding issues related to online safety on CPOMS

This policy will be reviewed every two years the Head Teacher. At every review, the policy will be shared with the governing board.

13. 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
- ICT and internet acceptable use policy
- Staff code of conduct/handbook

Acceptable Use Policy

Introduction

New technologies have become integral to the lives of children and young people in today's society, both within school and in their lives outside of school. This has been especially relevant due to the Covid-19 pandemic where children and staff were forced to work from home using online digital technologies. The internet and other digital information and communications technologies are powerful tools, which open up new opportunities for everyone. These technologies can stimulate discussion, and promote creativity and awareness of context to promote effective learning. They also bring opportunities for staff to be more creative and productive in their work. All users should have an entitlement to safe access to the internet and digital technologies at all times.

This agreement 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.
- School systems and users are protected from accidental or deliberate misuse that could put the security of the systems at risk.
- The provision of digital technologies to enhance learning is made possible through correct use
- Staff and volunteers are responsible users and stay safe while using the internet and other communications technologies for educational, personal and recreational use.
- School systems and users are protected from accidental or deliberate misuse that could put the security of the systems and users at risk.
- Staff are protected from potential risk in their use of technology in their everyday work.

The school will try to ensure that staff and volunteers will have good access to digital technology to enhance their work and learning opportunities for pupils learning. In return, staff and volunteers are expected to agree to be responsible users.

Appendix 1: EYFS and KS1 acceptable use agreement (pupils and parents/carers)

ACCEPTABLE USE OF THE SCHOOL'S ICT SYSTEMS AND INTERNET: AGREEMENT FOR PUPILS AND PARENTS/CARERS	
Name of pupil:	
Foundation Stage and Key Stage 1 To stay safe when we are using technology we **must** remember the following: If I'd like to use any devices- computers, tablets, laptops etc. - I will always ask a teacher or another trusted adult. When I'm using a device and I'm on the internet, I will only visit the website or webpage that my teacher has told me to visit. When I'm using a device, I will only open the app or any other piece of software that my teacher has asked me to open. I will make sure that I am careful and I will look after all the devices in my classroom and around the school. If I feel upset or worried about anything I see on-screen, then I **must** tell a teacher or trusted adult immediately. If I am unsure about anything that I am doing on a device, then I will ask a teacher or trusted adult for help. If I have got something wrong or something surprising happened on my screen, then I will ask a teacher or trusted adult for help. I will keep all my own passwords safe and I will never use somebody else's password. I will not share any personal information online including things like my real name, address, date of birth or school. I must **never** communicate with strangers online. I understand that if I do not follow these rules that I may not be allowed to use school devices in the future.	
Signed (pupil):	**Date:**

Appendix 2: KS2 acceptable use agreement (pupils and parents/carers)

ACCEPTABLE USE OF THE SCHOOL'S ICT SYSTEMS AND INTERNET: AGREEMENT FOR PUPILS AND PARENTS/CARERS
Name of pupil:

To stay safe when we are using technology we **must** remember the following:

I understand that for the safety of myself and others that the school will monitor my use of technology in the school on computers and other devices.

I understand that the school will contact my parents/carers if an adult at school is concerned about me or my use of technology.

I will keep my username and password safe and secure e.g. this means not writing them down or sharing them with others.

I will not use anyone else's username and password.

When I'm using a device, I will only open the app or any other piece of software that my teacher has asked me to open.

I will not open any links or attachments sent to my email account without checking with a trusted adult or teacher first.

I will only use school devices when a teacher or trusted adult has given me permission to do so.

I will make sure that I am careful and I will look after all the devices in my classroom and around the school.

I will notify a teacher or trusted adult if I notice that something on a device isn't working properly or is damaged in some way.

If I am unsure about anything that I am doing on a device, then I will ask a teacher or trusted adult for help.

If I have got something wrong or something surprising has happened on my screen, then I will ask a teacher or trusted adult for help.

If I feel upset or worried about anything that I see on screen, then I MUST tell a teacher or trusted adult.

If I see anything that I know is inappropriate on screen, then I MUST tell a teacher or trusted adult immediately.

When I communicate with other on email or any other messenger service, I will always be careful, kind, respectful, responsible and polite.

I will not post or share personal information about myself or others online e.g. names, phone numbers, addresses, school name, date of birth, phone numbers etc.

I will not send or share anything online or in a message that I know could make others feel upset.

I will be thoughtful about others' feelings when I communicate online.

I will not look up or save anything that I know could make others feel upset.

I must **never** communicate with strangers online.

I must **never meet** with strangers that have contacted me online- remember "Stranger Danger!"

If someone tries to contact me via any kind of message-e.g. email, game chat room, message service etc. - I will tell a trusted adult immediately.

I understand that if I do not follow these rules, or in any way behave unkindly or inappropriately with technology in school, I may not be allowed to use school devices in the future and my parents/carers will be informed.

Signed (pupil):	**Date:**

Appendix 3: Acceptable User Staff and Adult Agreement

Introduction

New technologies have become integral to the lives of children and young people in today's society, both within school and in their lives outside of school. The internet and other digital information and communications technologies are powerful tools, which open up new opportunities for everyone. These technologies can stimulate discussion, and promote creativity and awareness of context to promote effective learning. They also bring opportunities for staff to be more creative and productive in their work. All users should have an entitlement to safe access to the internet and digital technologies at all times.

This agreement is intended to ensure that:

- Staff and volunteers are responsible users and stay safe while using the internet and other communications technologies for educational, personal and recreational use.
- School systems and users are protected from accidental or deliberate misuse that could put the security of the systems and users at risk.
- Staff are protected from potential risk in their use of technology in their everyday work.

The school will try to ensure that staff and volunteers will have good access to digital technology to enhance their work and learning opportunities for pupils learning. In return, staff and volunteers are expected to agree to be responsible users.

Acceptable Use Agreement

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

For my professional and personal safety:

- I understand that the school will monitor my use of the school digital technology and communications systems.
- I understand that the rules set out in this agreement also apply to the use of these technologies (e.g. laptops, email, VLE etc.) out of school, and to the transfer of personal data (digital or paper based) out of school.
- I will not disclose my username or password to anyone else, nor will I try to use any other person's username and password. I understand that I should not write down or store a password where it is possible that someone may steal it.
- I will immediately report any illegal, inappropriate or harmful material or incident I become aware of to the appropriate person.

I will be professional in my communications and actions when using school ICT systems:

- I will not access, copy, remove or otherwise alter any other user's files, without their express permission.
- I will communicate with others in a professional manner, I will not use aggressive or inappropriate language and I appreciate that others may have different opinions.

- 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 not use my personal equipment to record these images, unless I have permission to do so. Where these images are published (e.g. on the school website/VLE) it will not be possible to identify by name, or other personal information, those who are featured.
- I will only use social networking sites in school in accordance with the school's policies.
- I will only communicate with 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.

The school and the local authority have the responsibility to provide safe and secure access to technologies and ensure the smooth running of the school:

- When I use my mobile devices (laptops/tablets/mobile phones/USB devices etc.) in school, I will follow the rules set out in this agreement, in the same way as if I was using school equipment. I will also follow any additional rules set by the school about such use. I will ensure that any such devices are protected by up to date anti-virus software and are free from viruses.
- I will not open any hyperlinks in emails or any attachments to emails, unless the source is known and trusted, 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 ensure that my data is regularly backed up, in accordance with relevant school policies.
- I will not try to upload, download or access any materials which are illegal (child sexual abuse images, criminally racist material, adult pornography covered by the Obscene Publications Act) or inappropriate or may cause harm/distress to others. I will not 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 not try (unless I have permission) to make large downloads or uploads that might take up internet capacity and prevent other users from being able to carry out their work.
- 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, unless this is allowed in school policies.
- I will not disable or cause any damage to school equipment, or the equipment belonging to others.
- I will only transport, hold, disclose or share personal information about myself or others, as outlined in the School/LA Personal Data Policy (or other relevant policy). Where digital personal data is transferred outside the secure local network, it must be encrypted. Paper based protected and restricted data must be held in lockable storage.
- I understand that data protection policy requires that any staff or 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.

When using the internet in my professional capacity or for school sanctioned personal use:

- I will ensure that I have permission to use the original work of others in my own work.
- Where work is protected by copyright, I will not download or distribute copies (including music and videos).

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

- I understand that this Acceptable Use Policy applies not only to my work and use of digital technology equipment in school, but also applies to my use of school systems and equipment off the premises and my use of personal equipment on the premises or in situations related to my employment by the school.
- I understand that if I fail to comply with this Acceptable Use Agreement, I could be subject to disciplinary action. This could include: a warning, a suspension, referral to Governors and/or the Local Authority and, in the event of illegal activities, and the involvement of the police.

I have read and understand the above and agree to use the school digital technology 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.

Staff/Student/Volunteer Name: .....

Signed: .....

Date: .....

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

ONLINE SAFETY TRAINING NEEDS AUDIT	
Name of staff member/volunteer:	**Date**:
Question	**Yes/No (add comments if necessary)**
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?	

Sept 2024

Review: Sept 2026