

OUR LADY'S CATHOLIC PRIMARY SCHOOL



We ASPIRE that through the love of Jesus everyone should
"have life and have it to the full".

John 10:10

ONLINE SAFETY POLICY

Reviewed by: <i>Headteacher</i>	Approved by: <i>Governing Body</i>
Policy Date: <i>February 2026</i>	Next Review Date: <i>Spring 2027</i>
Review Frequency: <i>Annually</i>	



'have life and have it to the full'

Introduction

Mobile and smart devices are evolving and being updated on an almost daily basis and are now an integral part of life for both adults and children alike. These are powerful tools, which when used properly, can open up new opportunities for everyone. The use of these exciting and innovative tools in school and at home has been shown, when used effectively, to raise educational standards and promote pupil achievement.

We are required to ensure that children learn how to use these technologies safely and always have access to safe internet. This is addressed as part of a wider duty of care to which all who work in schools are bound.

At Our Lady's Catholic Primary School, we are committed to providing a safe, inclusive and nurturing environment in which every member of our community is known, valued and loved. Inspired by the teachings of Jesus Christ and guided by our mission that all may "have life and have it to the full" (John 10:10), we seek to create a school culture where each child can flourish academically, socially, emotionally and spiritually.

1. Aims

Our school aims to:

- Have robust processes in place to ensure the online safety of pupils, staff, volunteers and governors
- Identify and support groups of pupils who may be at greater risk of harm online
- Deliver an effective approach to online safety that protects and educates the whole school community in its use of technology, including mobile and smart technology
- Establish clear procedures to identify, respond to and escalate online safety incidents where appropriate
- Promote a culture of safe, responsible and respectful use of technology
- Ensure that online safety remains a key part of the school's wider safeguarding responsibilities

The 4 Key Categories of Risk

Our approach to online safety is based on addressing the following four categories of risk:

Content

Being exposed to illegal, inappropriate or harmful content, including:

- pornography
- misinformation and disinformation (including fake news)
- conspiracy theories
- racist content
- misogynistic content



'have life and have it to the full'

- self-harm content
- suicide-related content
- antisemitic content
- radicalisation
- extremism
- harmful online challenges
- inappropriate AI-generated content

Contact

Being subjected to harmful online interactions with others, including:

- peer-to-peer pressure
- online bullying
- sexual harassment
- coercion
- commercial advertising
- adults posing as children or young people
- grooming for sexual, criminal or financial exploitation
- online abuse or manipulation

Conduct

Personal online behaviour that increases the likelihood of, or causes, harm, including:

- making, sending or receiving explicit images
- consensual and non-consensual sharing of nudes and semi-nudes
- sharing harmful or explicit content
- sexualised messaging
- image sharing abuse
- participating in harmful online challenges
- inappropriate use of social media
- behaviour that places pupils at risk of exploitation or abuse online

Commerce

Risks such as:

- online gambling



'have life and have it to the full'

- phishing
- scams
- inappropriate advertising
- financial exploitation
- fraudulent online activity

2. Legislation and guidance

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

- [Teaching online safety](#)
- [Meeting digital and technology standards](#)
- [Preventing and tackling bullying](#) and [cyber-bullying: advice for headteachers and school staff](#)
- [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 make sure all staff undergo online safety training as part of child protection and safeguarding training, and ensure staff understand their expectations, roles and responsibilities around filtering and monitoring.

The governing board will also make sure all staff receive regular online safety updates (via email, e-bulletins and staff meetings), as required and at least annually, to ensure they are continually provided with the relevant skills and knowledge to effectively safeguard children.

The governing board will co-ordinate regular meetings with appropriate staff to discuss online safety and requirements for training and monitor online safety logs as provided by the designated safeguarding lead (DSL).



'have life and have it to the full'

The governing board will make sure that the school teaches pupils how to keep themselves and others safe, including online.

The governing board will make sure that the school has appropriate filtering and monitoring systems in place on school devices and school networks and will regularly review their effectiveness. The board will review the [DfE's filtering and monitoring standards](#), and discuss with IT staff and service providers what needs to be done to support the school in meeting the standards, which include:

- Identifying and assigning roles and responsibilities to manage filtering and monitoring systems
- Reviewing filtering and monitoring provisions at least annually
- Blocking harmful and inappropriate content without unreasonably impacting teaching and learning
- Having effective monitoring strategies in place that meet the school's safeguarding needs

All governors will:

- Make sure 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)
- Make sure that online safety is a running and interrelated theme when devising and implementing the whole-school approach to safeguarding and related policies and/or procedures
- Make sure that, where necessary, teaching about safeguarding, including online safety, is adapted for vulnerable children, victims of abuse and some pupils with special educational needs and/or disabilities (SEND). This is because of the importance of recognising that a 'one size fits all' approach may not be appropriate for all children in all situations, and a more personalised or contextualised approach may often be more suitable

3.2 The headteacher

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

3.3 The designated safeguarding lead (DSL)

Details of the school's designated safeguarding leads (DSL) 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 making sure that staff understand this policy and that it is being implemented consistently throughout the school
- Working with the headteacher and governing board to review this policy and make sure the procedures and implementation are updated and reviewed regularly



'have life and have it to the full'

- Taking the lead on understanding the filtering and monitoring systems and processes in place on school devices and school networks
- Providing governors with assurance that filtering and monitoring systems are working effectively and reviewed regularly
- Working with the ICT manager to make sure the appropriate systems and processes are in place
- Working with the headteacher, ICT manager and other staff, as necessary, to address any online safety issues or incidents
- Managing all online safety issues and incidents in line with the school's child protection policy
- Responding to safeguarding concerns identified by filtering and monitoring
- Making sure that any online safety incidents are logged (see appendix 5) and dealt with appropriately in line with this policy
- Making sure 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
- Undertaking annual risk assessments that consider and reflect the risks pupils face
- Providing regular safeguarding and child protection updates, including online safety, to all staff, at least annually, in order to continue to provide them with relevant skills and knowledge to safeguard effectively

This list is not intended to be exhaustive.

3.4 The ICT manager

The ICT manager is responsible for:

- Putting in place an appropriate level of security protection procedures, such as filtering and monitoring systems on school devices and school networks, which are reviewed and updated at least annually to assess effectiveness and make sure pupils are kept safe from potentially harmful and inappropriate content and contact online while at school, including terrorist and extremist material
- Making sure that the school's ICT systems are secure and protected against viruses and malware, and that such safety mechanisms are updated regularly



'have life and have it to the full'

- Conducting a full security check and monitoring the school's ICT systems on a weekly basis.
- Blocking access to potentially dangerous sites and, where possible, preventing the downloading of potentially dangerous files
- Making sure that any online safety incidents are logged (see appendix 5) and dealt with appropriately in line with this policy
- Making sure 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.

3.5 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 making sure that pupils follow the school's terms on acceptable use (appendices 1 and 2)
- Knowing that the DSL is responsible for the filtering and monitoring systems and processes and being aware of how to report any incidents of those systems or processes failing.
- Following the correct procedures if they need to bypass the filtering and monitoring systems for educational purposes.
- Working with the DSL to make sure that any online safety incidents are logged (see appendix 5) and dealt with appropriately in line with this policy.
- Making sure that any incidents of cyber-bullying are dealt with appropriately in line with the school behaviour policy.
- Responding appropriately to all reports and concerns about sexual violence and/or harassment, both online and offline, and maintaining an attitude of 'it could happen here'.
- This list is not intended to be exhaustive.

3.6 Parents/carers

Parents/carers are expected to:

- Notify a member of staff or the headteacher of any concerns or queries regarding this policy.
- Make sure that 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/carers can seek further guidance on keeping children safe online from the following organisations and websites:

- What are the issues? – [UK Safer Internet Centre](#)



'have life and have it to the full'

- Help and advice for parents/carers – [Childnet](#)
- Parents and carers resource sheet – [Childnet](#)

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 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

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

All schools have to teach:

- [Relationships education and health education](#) in primary schools

In **Key Stage (KS) 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 (KS) 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
- Be discerning in evaluating digital content

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

- That people should be respectful in online interactions, and that the same principles apply to online relationships as to face-to-face relationships, including where people are anonymous. For example, the importance of avoiding putting pressure on others to share information and images online, and strategies for resisting peer pressure
- How to critically evaluate their online relationships and sources of information, including awareness of the risks associated with people they have never met. For example, that people sometimes behave differently online, including pretending to be someone else, or pretending to be a child, and that this can lead to dangerous situations. How to recognise harmful content or harmful contact, and how to report this
- That there is a minimum age for joining social media sites (currently 13), which protects children from inappropriate content or unsafe contact with older social media users, who may be strangers, including other children and adults
- The importance of exercising caution about sharing any information about themselves online. Understanding the importance of privacy and location settings to protect information online



'have life and have it to the full'

- Online risks, including that any material provided online might be circulated, and that once a picture or words has been circulated there is no way of deleting it everywhere and no control over where it ends up
- That the internet contains a lot of content that can be inappropriate and upsetting for children, and where to go for advice and support when they feel worried or concerned about something they have seen or engaged with online
- Pupils will be reminded regularly how to report online safety concerns both in school and at home, including speaking to trusted adults, reporting concerns to school staff, and accessing appropriate online reporting tools where appropriate.

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

Where necessary, teaching about safeguarding, including online safety, will be adapted for vulnerable children, victims of abuse and some pupils with SEND.

4.2 Pupils will be taught practical cyber security skills

All pupils will receive age-appropriate training on safe internet use, including:

- Methods that hackers use to trick people into disclosing personal information
- Password security
- Social engineering
- The risks of removable storage devices (e.g. USBs)
- Multi-factor authentication
- How to report a cyber incident or attack
- How to report a personal data breach

Pupils will also receive age-appropriate education on online sexual harassment, harmful online challenges, coercion, image sharing abuse and inappropriate online behaviour, including how to seek help and report concerns.

5. Educating parents/carers about online safety

The school will raise parents/carers' awareness of internet safety in letters or other communications home, and in information via our website. This policy will also be shared with parents/carers.

Parents/carers will also receive updates regarding emerging online risks, including artificial intelligence, social media trends, gaming risks, harmful online content and other developing online safety concerns.

Online safety will also be covered during parents' evenings.

The school will let parents/carers know:



'have life and have it to the full'

- What systems the school uses to filter and monitor online use
- What their children are being asked to do online, including the sites they will be asked to access and who from the school (if anyone) their child will be interacting with online

If parents/carers 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 1 person or group by another person or group, where the relationship involves an imbalance of power. (See also the school behaviour policy.)

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 encourage them 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 classes.

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/carers so 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 report the incident and provide the relevant material to the police as soon as is reasonably practicable, if they have reasonable grounds to suspect that possessing that material is illegal. They will also work with external services if it is deemed necessary to do so.

6.3 Examining electronic devices

The headteacher, and any member of staff authorised to do so by the headteacher, can carry out a search and confiscate any electronic device that they have reasonable grounds for suspecting:

- Poses a risk to staff or pupils, and/or



'have life and have it to the full'

- Is identified in the school rules as a banned item for which a search can be carried out, and/or
- Is evidence in relation to an offence

Before a search, if the authorised staff member is satisfied that they have reasonable grounds for suspecting any of the above, they will also:

- Assess how urgent the search is and consider the risk to other pupils and staff. If the search is not urgent, they will seek advice from the headteacher or another DSL.
- Explain to the pupil why they are being searched, and how the search will happen; and give them the opportunity to ask questions about it
- Seek the pupil's co-operation

Authorised staff members may examine, and in exceptional circumstances erase, any data or files on an electronic device that they have confiscated where they believe there is a 'good reason' to do so.

When deciding whether there is a 'good reason' to examine data or files on an electronic device, the staff member should reasonably suspect that the device has, or could be used to:

- Cause harm, and/or
- Undermine the safe environment of the school or disrupt teaching, and/or
- Commit an offence

If inappropriate material is found on the device, it is up to the headteacher or DSL to decide on a suitable response. If there are images, data or files on the device that staff reasonably suspect are likely to put a person at risk, they will first consider the appropriate safeguarding response.

When deciding whether there is a good reason to erase data or files from a device, staff members will consider if the material may constitute evidence relating to a suspected offence. In these instances, they will not delete the material, and the device will be handed to the police as soon as reasonably practicable. If the material is not suspected to be evidence in relation to an offence, staff members may delete it if:

- They reasonably suspect that its continued existence is likely to cause harm to any person, and/or
- The pupil and/or the parent/carers refuses to delete the material themselves

If a staff member **suspects** a device **may** contain an indecent image of a child (also known as a nude or semi-nude image), they will:

- **Not** view the image
- Confiscate the device and report the incident to the DSL (or equivalent) immediately, who will decide what to do next. The DSL will make the decision in line with the DfE's latest guidance on [screening, searching and confiscation](#) and the UK Council for Internet Safety (UKCIS) guidance on [sharing nudes and semi-nudes: advice for education settings working with children and young people](#)

Any searching of pupils will be carried out in line with:



'have life and have it to the full'

- > The DfE's latest guidance on [searching, screening and confiscation](#)
- > UKCIS guidance on [sharing nudes and semi-nudes: advice for education settings working with children and young people](#)
- > Our behaviour policy

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

6.4 Artificial intelligence (AI)

Generative artificial intelligence tools such as ChatGPT, Google Gemini and similar platforms are becoming increasingly accessible to staff, pupils and parents/carers.

Our Lady's Catholic Primary School recognises that artificial intelligence can support teaching and learning when used appropriately. However, it may also present safeguarding, online safety and data protection risks.

Potential risks may include:

- misinformation and disinformation
- inaccurate or misleading information
- deepfakes and manipulated images, audio or videos
- cyberbullying
- inappropriate or harmful content
- privacy breaches
- misuse of personal information
- plagiarism or misuse of schoolwork

The school recognises that AI may also be used to bully, harm or exploit others, including through the creation or sharing of deepfake content. Any misuse of AI to harm pupils, staff or members of the school community will be taken seriously and managed in line with the school's behaviour, safeguarding and child protection policies.

Staff must not input confidential, personal or safeguarding-related pupil information into AI platforms.

Staff must carry out appropriate risk assessments before introducing new AI tools and ensure that any AI used within school is age-appropriate, safe and supports learning effectively.

The school will follow Department for Education Generative AI product safety expectations guidance.

Filtering and monitoring systems will continue to be reviewed to ensure pupils are protected when using AI tools, and any safeguarding concerns relating to AI use will be reported to the Designated Safeguarding Lead (DSL).



'have life and have it to the full'

7. Acceptable use of the internet in school

All pupils, parents/carers, 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 to 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 and restrict access through filtering systems where appropriate.

More information is set out in the acceptable use agreements in appendices 1 to 3.

8. Pupils using mobile devices in school

Only pupils in Years 5 and 6 may bring mobile devices into school, but are not permitted to use them during:

- Lessons
- Clubs before or after school, or any other activities or trips organised by the school

Mobile phones must be handed into the teacher at the start of the day and will be handed back to the child as they leave at the end of the 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.

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 can be made up of [3 random words](#), in combination with numbers and special characters if required, or generated by a password manager
- 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 by promptly installing the latest updates

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



'have life and have it to the full'

Work devices must be used solely for work activities.

If staff have any concerns regarding the security of their device, they must seek advice from the Designated Safeguarding Lead (DSL), Headteacher, Online Safety Lead or the school's IT technician, where appropriate.

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. 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, the internet or misuses a personal device where the action constitutes misconduct, the matter will be dealt with in accordance with the 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 that involve illegal activity or content, or otherwise serious incidents, should be reported to the police.

11. Training for staff, governors and volunteers

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).

By way of this training, all staff will be made aware that:

- Technology is a significant component in many safeguarding and wellbeing issues, and that children are at risk of online abuse
- Children can abuse their peers online through:
 - Abusive, threatening, harassing and misogynistic messages
 - Non-consensual sharing of indecent nude and semi-nude images and/or videos, especially around chat groups
 - Sharing of abusive images and pornography, to those who don't want to receive such content
- Physical abuse, sexual violence and initiation/hazing type violence can all contain an online element

Training will also help staff:

- Develop better awareness to assist in spotting the signs and symptoms of online abuse
- Develop the ability to ensure pupils can recognise dangers and risks in online activity and can weigh up the risks



'have life and have it to the full'

- Develop the ability to influence pupils to make the healthiest long-term choices and keep them safe from harm in the short term

The DSL and Deputy DSLs 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. An incident report log can be found in appendix 5.

This policy will be reviewed every year by the Online Safety Lead. At every review, the policy will be shared with the governing board. The review (such as the one available [here](#)) will be supported by an annual risk assessment that considers and reflects the risks pupils face online. This is important because technology, and the risks and harms related to it, evolve and change rapidly.

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



'have life and have it to the full'

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:

When I use the school's ICT systems (like computers) and get onto the internet in school I will:

- Ask a teacher or adult if I can do so before using them
- Only use websites that a teacher or adult has told me or allowed me to use
- Tell my teacher immediately if:
 - I select a website by mistake
 - I receive messages from people I don't know
 - I find anything that may upset or harm me or my friends
- Use school computers for schoolwork only
- Be kind to others and not upset or be rude to them
- Look after the school ICT equipment and tell a teacher straight away if something is broken or not working properly
- Only use the username and password I have been given
- Try my hardest to remember my username and password
- Never share my password with anyone, including my friends
- Never give my personal information (my name, address or telephone numbers) to anyone without the permission of my teacher or parent/carers
- Save my work on the school network
- Check with my teacher before I print anything
- Log off or shut down a computer or other device when I have finished using it

I agree that the school will monitor the websites I visit and that there will be consequences if I don't follow the rules.

Signed (pupil):

Date:

Parent/carers agreement: I agree that my child can use the school's ICT systems and internet when appropriately supervised by a member of school staff. I agree to the conditions set out above for pupils using the school's ICT systems and internet, and will make sure my child understands these.

Signed (parent/carers):

Date:



'have life and have it to the full'

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:

I will read and follow the rules in the acceptable use agreement policy.

When I use the school's ICT systems (like computers) and get onto the internet in school I will:

- Always use the school's ICT systems and the internet responsibly and for educational purposes only
- Only use them when a teacher is present, or with a teacher's permission
- Keep my usernames and passwords safe and not share these with others
- Keep my private information safe at all times and not give my name, address or telephone number to anyone without the permission of my teacher or parent/carer
- Tell a teacher (or sensible adult) immediately if I find any material that might upset, distress or harm me or others
- Always log off or shut down a computer when I've finished working on it

I will not:

- Access any inappropriate websites including: social networking sites, chat rooms and gaming sites unless my teacher has expressly allowed this as part of a learning activity
- Open any attachments in emails, or follow any links in emails, without first checking with a teacher
- Use any inappropriate language when communicating online, including in emails
- Create, link to or post any material that is pornographic, offensive, obscene or otherwise inappropriate
- Log in to the school's network using someone else's details
- Arrange to meet anyone offline without first consulting my parent/carer, or without adult supervision

If I bring a personal mobile phone or other personal electronic device into school:

- I will not use it during lessons, tutor group time, clubs or other activities organised by the school, without a teacher's permission
- I will use it responsibly, and will not access any inappropriate websites or other inappropriate material or use inappropriate language when communicating online

I agree that the school will monitor the websites I visit and that there will be consequences if I don't follow the rules.

Signed (pupil):

Date:

Parent/carer's agreement: I agree that my child can use the school's ICT systems and internet when appropriately supervised by a member of school staff. I agree to the conditions set out above for pupils using the school's ICT systems and internet, and for using personal electronic devices in school, and will make sure my child understands these.

Signed (parent/carer):

Date:



'have life and have it to the full'

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

ACCEPTABLE USE OF THE SCHOOL'S ICT SYSTEMS AND INTERNET: AGREEMENT FOR STAFF, GOVERNORS, VOLUNTEERS AND VISITORS

Name of staff member/governor/volunteer/visitor:

When using school ICT systems, devices, online services or internet access, I will not:

- Access, create, share, link to, send or deliberately search for inappropriate, illegal or harmful material, including violent, criminal or pornographic content.
- Use school systems, accounts or devices in a way that could compromise safeguarding, security, confidentiality or the reputation of the school.
- Use social media, messaging or online communication in a way that breaches professional boundaries, confidentiality or the Staff Code of Conduct.
- Use improper, discriminatory, abusive or unprofessional language in emails, messages or other online communications.
- Install unauthorised software, browser extensions or apps, connect unauthorised hardware, or use unapproved cloud services where school information is involved.
- Share passwords, authentication codes or accounts, allow another person to use my login, or use another person's credentials.
- Attempt to bypass filtering, monitoring, security controls or access restrictions.
- Access, alter, download, copy or share information that I am not authorised to access or use.
- Share confidential, personal, safeguarding or sensitive information about pupils, staff, families or the school except through authorised systems and for a legitimate professional purpose.
- Use personal email accounts, personal cloud storage or unauthorised personal devices to store or transfer school information unless specifically authorised by the school.
- Take, store, publish or share photographs, video or audio recordings of pupils except for an authorised school purpose and in accordance with school procedures and permissions.
- Use school systems to promote a private business or for significant personal or commercial activity unless expressly authorised.



'have life and have it to the full'

ACCEPTABLE USE OF THE SCHOOL'S ICT SYSTEMS AND INTERNET: AGREEMENT FOR STAFF, GOVERNORS, VOLUNTEERS AND VISITORS

I understand and agree that I will:

- Use school ICT systems, devices and online services responsibly and primarily for educational purposes or to fulfil the duties of my role.
- Keep passwords secure, use multi-factor authentication (MFA) where provided, lock devices when unattended and take reasonable steps to prevent unauthorised access.
- Be alert to phishing, suspicious links, attachments, unexpected login prompts and other cyber-security risks, and report suspected phishing, malware or compromised accounts promptly.
- Report lost or stolen devices, misdirected emails, accidental disclosures, suspected data breaches, unauthorised access or other information-security incidents immediately in accordance with the school's Data Protection Policy and reporting arrangements.
- Keep school information securely stored and only use authorised systems, apps and services for school data.
- Follow the school's rules on social media and maintain professional boundaries online; I will not post or share confidential school information or identifiable pupil information/images without proper authority.
- Only use photography, video or audio recording for an authorised school purpose, using approved devices/systems and following the school's consent, safeguarding and data-protection procedures.
- Report to the DSL and appropriate ICT lead if a pupil tells me they have encountered material that may upset, distress or harm them or others, or if I encounter such material myself.
- Not investigate safeguarding content myself beyond what is necessary to report the concern; I will preserve evidence only as directed by the DSL or other authorised lead.
- Accept that the school may filter and monitor use of its ICT facilities, systems, networks and internet access in accordance with school policy and applicable law.
- Promote responsible use by pupils in my care and report concerns about misuse, unsafe behaviour or attempts to bypass school controls.

AI and generative AI

- Use only AI/generative-AI tools that the school has authorised for the intended purpose.
- Never enter identifiable pupil or staff information, safeguarding information, special-category data, confidential school information or assessment material into an AI tool unless the school has explicitly approved that specific use and the relevant data-protection arrangements permit it.
- Check AI-generated content for accuracy, bias, appropriateness, copyright/provenance concerns and safeguarding risk before using or sharing it; professional judgement and accountability remain with me.
- Be transparent about material AI use where required by school procedures and never use AI to impersonate another person, fabricate evidence or circumvent professional responsibilities.

I understand that breaches of this agreement may be dealt with under the school's safeguarding, data protection, disciplinary or other relevant procedures.

Signed (staff member/governor/volunteer/visitor):

Date:



'have life and have it to the full'

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?	
Are you aware of the ways pupils can abuse their peers online?	
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/carers?	
Are you familiar with the filtering and monitoring systems on the school's devices and networks?	
Do you understand your role and responsibilities in relation to filtering and monitoring?	
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?	



'have life and have it to the full'

Appendix 5: online safety incident report log

ONLINE SAFETY INCIDENT LOG				
Date	Where the incident took place	Description of the incident	Action taken	Name and signature of staff member recording the incident