# Online Safety Policy

| | |
|---|---|
| Approved by: | Directors |
| Last reviewed on: | February 2026 |
| Review frequency | Annually |
| Next review due by: | February 2027 |
| Ownership | Company Secretary |

**Setting:** St Brendan's Catholic Primary School

**Designated Safeguarding Lead:** Kim Dixon

**Safeguarding Link Governor:** Brian Sweeney

**Safeguarding Director:** Joe Burns JBurns@olicatschools.org

# Online Safety Policy

## Contents

# Online Safety Policy

## Statement of intent

St Brendan's Catholic Primary School understands that using online services is an important aspect of raising educational standards, promoting pupil[1] achievement, and enhancing teaching and learning. The use of online services is embedded throughout the school; therefore, there are a number of controls in place to ensure the safety of pupils and staff.

The breadth of issues classified within online safety is considerable, but they can be categorised into four areas of risk:

- **Content**: Being exposed to illegal, inappropriate or harmful material, e.g. pornography, fake news, self-harm and suicide, and discriminatory or extremist views.
- **Contact**: Being subjected to harmful online interaction with other users, e.g. peer pressure, commercial advertising, and adults posing as children or young adults with the intention to groom or exploit children.
- **Conduct**: Personal online behaviour that increases the likelihood of, or causes, harm, e.g. sending and receiving explicit messages, and cyberbullying.
- **Commerce**: Risks such as online gambling, inappropriate advertising, phishing and/or financial scams.

The measures implemented to protect pupils and staff revolve around these areas of risk. Our school has created this policy with the aim of ensuring appropriate and safe use of the internet and other digital technology devices by all pupils and staff.

## Legal framework

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 in schools
- Preventing and tackling bullying and cyber-bullying: advice for headteachers and school staff
- [Relationships and sex education (RSE) and health education – remove if not applicable, see section 4]
- 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.

This policy complies with our funding agreement and articles of association.

This policy has due regard to all relevant legislation and guidance including, but not limited to, the following:

- Voyeurism (Offences) Act 2019
- The UK General Data Protection Regulation (UK GDPR)
- Data Protection Act 2018
- DfE (2024) 'Filtering and monitoring standards for schools and colleges'
- DfE (2021) 'Harmful online challenges and online hoaxes'
- DfE (2024) 'Keeping children safe in education 2024'

[1] For the purposes of this policy, 'pupil' refers to all age ranges educated within OLICAT

- DfE (2023) 'Teaching online safety in school'
- DfE (2022) 'Searching, screening and confiscation'
- DfE (2023) 'Generative artificial intelligence in education'
- Department for Digital, Culture, Media and Sport and UK Council for Internet Safety (2020) 'Sharing nudes and semi-nudes: advice for education settings working with children and young people'
- UK Council for Child Internet Safety (2020) 'Education for a Connected World – 2020 edition'
- National Cyber Security Centre (2020) 'Small Business Guide: Cyber Security'

This policy operates in conjunction with the following school policies:

- Device User Agreement
- Remote Education Policy
- Anti-Bullying Policy
- Safeguarding Policy (OLICAT)
- Child-on-child Abuse Policy
- Behaviour Policy
- Managing Allegations of Abuse Against Staff Policy (OLICAT)
- *Cyber-security Policy*
- Critical Incident / Emergency Plan
- Staff Code of Conduct (OLICAT)
- Disciplinary Policy (OLICAT)
- Data Protection (GDPR) Policy (OLICAT)

## Roles and responsibilities

The trust board will be responsible for:

- OLICAT has strategic leadership responsibility for the academy's safeguarding arrangements, and there is a whole academy approach to safeguarding (this includes online safety)
- The trust board delegate responsibility for the monitoring of the implementation of this policy to the local academy committee
- Ensuring the timely review and approval of this policy template
- Ensuring that online safety is a running and interrelated theme throughout the trust's policies and procedures
- Ensuring that the relevant central staff work with the DSLs, SLTs and IT team to procure appropriate filtering and monitoring systems.
- Through delegation to the Central Team ensure that the filtering provider is:
    - A member of the Internet Watch Foundation (IWF)
    - Signed up to Counter-Terrorism Internet Referral Unit list (CTIRU)
    - Blocking access to illegal content including child sexual abuse material (CSAM)
- Through delegation to the Central Team ensure that filtering and monitoring systems are operational, maintained, up to date and applied to all:
    - Users including guest accounts
    - School owned devices
    - Devices using the school broadband connection

The local academy committee will be responsible for:

- Ensuring that this policy is implemented affectively
- Ensuring there is a senior member of the leadership team who is designated to take lead responsibility for dealing with safeguarding and child protection (the "Designated Safeguarding Lead") and there is

always cover for this role (at least one deputy) with appropriate arrangements for before/after school and out of term activities

- Ensuring the DSL's remit covers online safety (including filtering and monitoring)
- Ensuring that a member of the local academy committee is responsible for ensuring that online safety requirements (including filtering and monitoring standards) are being met – this may be the Safeguarding Link Governor or another member of the board with an interest
- Ensuring their own knowledge of online safety issues is up-to-date
- Ensuring all staff undergo safeguarding and child protection training, including online safety, at induction and at regular intervals
- Ensuring that there are appropriate filtering and monitoring systems in place and that it is meeting the DfE's Filtering and monitoring standards for schools and colleges
- Ensuring that 'over blocking' does not lead to unreasonable restrictions as to what pupils can be taught with regards to online teaching and safeguarding
- Ensuring that the effectiveness of filtering and monitoring systems is reviewed at least annually in liaison with ICT staff and service providers, and review the results
- Ensuring that the SLT and other relevant staff have an awareness and understanding of the filtering and monitoring and device monitoring provisions in place, and manage them effectively and know how to escalate concerns when identified
- Supporting the SLT to review the effectiveness of the monitoring strategies and reporting processes
- Ensuring that all relevant school policies have an effective approach to planning for, and responding to, online challenges and hoaxes embedded within them.

The Head (in conjunction with the SLT) will be responsible for:

- Ensuring that online safety is a running and interrelated theme throughout the school's policies and procedures, including in those related to the curriculum, teacher training and safeguarding
- Supporting the DSL and the deputy DSL by ensuring they have enough time and resources to carry out their responsibilities in relation to online safety
- Ensuring staff receive regular, up-to-date and appropriate online safety training and information as part of their induction and safeguarding training
- Ensuring that the DSL works in conjunction with the trust and ICT technicians to procure an adequate filtering and monitoring system which meets legal standards
- Ensuring that effective device monitoring is in place which meets the legal standards and the risk profile of the school including risk assessing what filtering and monitoring systems are required
- Ensuring online safety practices are audited and evaluated, and review the effectiveness of the monitoring strategies and reporting processes
- Organising engagement with parents to keep them up-to-date with current online safety issues and how the school is keeping pupils safe
- Working with the DSL and ICT technicians to conduct termly light-touch reviews of the effectiveness of this policy.

The DSL will be responsible for:

- Taking the lead responsibility for safeguarding and online safety, which includes overseeing and acting on:
    - filtering and monitoring
    - safeguarding concerns
    - checks to filtering and monitoring systems
- Undertaking training so they understand the risks associated with online safety and can recognise additional risks that pupils with SEND face online
- Liaising with relevant members of staff on online safety matters, e.g. the SENCO and ICT technicians

- Ensuring online safety is recognised as part of the school's safeguarding responsibilities and that a coordinated approach is implemented
- Ensuring safeguarding is considered in the school's approach to remote learning
- Establishing a procedure for reporting online safety incidents and inappropriate internet use, both by pupils and staff, and ensuring all members of the school community understand this procedure
- Working with the Head and ICT technicians to risk assess what filtering and monitoring systems are required
- Understanding the filtering and monitoring processes in place at the school
- Ensuring that specific roles and responsibilities are identified and assigned to manage filtering and monitoring systems and to ensure they meet the school's safeguarding needs
- Ensuring that all safeguarding training given to staff includes an understanding of the expectations, roles and responsibilities in relation to filtering and monitoring systems at the school
- Maintaining records of reported online safety concerns as well as the actions taken in response to concerns
- Monitoring online safety incidents to identify trends and any gaps in the school's provision, and using this data to update the school's procedures
- Reporting to the local committee of the board about online safety on a regular basis
- Working with the Head and ICT technicians to conduct termly light-touch reviews of the effectiveness of this policy
- Working with the trust central staff to update this policy annually.

ICT technicians will be responsible for and procedures

- Implementing appropriate technical measures as directed by the trust and school
- Working with the Head and DSL to risk assess what filtering and monitoring systems are required
- Ensure that the filtering system:
    - Filter all internet feeds, including any backup connections
    - Is age and ability appropriate for the users, and be suitable for educational settings (in conjunction with the DSL)
    - Is appropriate for the number of pupils using the network, how often pupils access the network and proportional in cost compared to risk
    - Handle multilingual web content, images, common misspellings and abbreviations
    - Identify technologies and techniques that allow users to get around the filtering such as VPNs and proxy services and block them
    - Provide alerts when any web content has been blocked
    - Provide filtering on mobile or app technologies (where necessary)
- Checking that they are meeting the requirements for broadband internet standards and cyber security standards
- Ensuring filtering and monitoring reports are available and accessible to the DSL/school team
- Completing actions following concerns or checks to systems
- Working with the DSL and Head to conduct termly light-touch reviews of the effectiveness this policy.

The Head, SLT, DSL and ICT team will all work together to:

- Procure systems (in conjunction with the trust)
- Identify risk
- Carry out reviews (at least annually)
- Carry out checks

All staff members will be responsible for:

- Taking responsibility for the security of ICT systems and electronic data they use or have access to
- Modelling good online behaviours

- Maintaining a professional level of conduct in their personal use of technology
- Having an awareness of online safety issues and ensuring they are familiar with, and understand, the indicators that pupils may be unsafe online
- Providing effective supervision
- Taking steps to maintain awareness of how devices are being used by pupils
- Reporting if they:
    - Have a safeguarding concern to DSL as outlined in the safeguarding policy.
    - Witness or suspect unsuitable material has been accessed
    - Can access unsuitable material.
    - Are teaching topics which could create unusual activity on the filtering logs
    - Believe there is a failure in the software or abuse of the system
    - Believe there are perceived unreasonable restrictions that affect teaching and learning or administrative tasks
    - Notice abbreviations or misspellings that allow access to restricted material
- Where relevant to their role, ensuring online safety is embedded in their teaching of the curriculum.

Pupils will be responsible for:

- Adhering to the Acceptable Use Agreement (Appendix A) and other relevant policies
- Seeking help from school staff if they are concerned about something they or a peer have experienced online
- Reporting online safety incidents and concerns in line with the procedures within this policy.

## Managing online safety

All staff will be aware that technology is a significant component in many safeguarding and wellbeing issues affecting young people, particularly owing to the rise of social media and the increased prevalence of children using the internet.

The DSL has overall responsibility for the school's approach to online safety, with support from deputies and the Head where appropriate, and will ensure that there are strong processes in place to handle any concerns about pupils' safety online. The DSL should liaise with the police or children's social care services for support responding to harmful online sexual behaviour.

The importance of online safety is integrated across all school operations in the following ways:

- Staff and governors receive regular training
- Staff receive regular email updates and training via our Handsam system regarding online safety information and any changes to online safety guidance or legislation.
- Online safety is integrated into learning throughout the curriculum via both our computing (Kapow)and PSHE scheme (Ten:Ten)
- Online safety is incorporated into our SMSC calendar with assemblies and focus events (internet safety day) throughout the year.
- Workshop are undertaken on whole class and individual levels using resources from Project evolve should the children require any additional learning e.g In the event of a emerging viral trend that may not be covered in our current online safety curriculum.

**Handling online safety concerns**

Any disclosures made by pupils to staff members about online abuse, harassment or exploitation, whether they are the victim or disclosing on behalf of another child, will be handled in line with the school's Safeguarding Policy.

Staff will:

- Be aware that harmful online sexual behaviour can progress on a continuum, and appropriate and early intervention can prevent abusive behaviour in the future
- Acknowledge that pupils displaying this type of behaviour are often victims of abuse themselves and should be suitably supported
- Not promise confidentiality
- Report concerns about a pupil's online behaviour to the DSL as outlined in the safeguarding policy.

The DSL and other appropriate staff members will:

- Not promise confidentiality, and information may be still shared lawfully, for example, if the DSL decides that there is a legal basis under UK GDPR such as the public task basis whereby it is in the public interest to share the information. If the decision is made to report abuse to children's social care or the police against the victim's wishes, this must be handled extremely carefully – the reasons for sharing the information should be explained to the victim and appropriate specialised support should be offered
- Investigate concerns raised about a pupil's online behaviour with relevant staff members, e.g. the Head and ICT technicians, and mange concerns in accordance with the relevant policies depending on their nature, e.g. the school Behaviour Policy and Safeguarding Policy
- Meet with the victim's parents to discuss the safeguarding measures that are being put in place to support their child and how the report will progress

Concerns regarding a staff member's online behaviour are reported to the Head, who decides on the best course of action in line with the relevant policies. If the concern is about the Head, it is reported to the Strategic Executive Lead of OLICAT.

Where there is a concern that illegal activity has taken place, the Head or DSL should contact the police.

The school should avoid unnecessarily criminalising pupils, e.g. calling the police, where criminal behaviour is thought to be inadvertent and as a result of ignorance or normal developmental curiosity, e.g. a pupil has taken and distributed indecent imagery of themselves. The DSL will decide in which cases this response is appropriate and will manage such cases in line with the school's Safeguarding Policy.

All online safety incidents and the school's response must be recorded by the safeguarding team or appropriate staff.

## Online safety training for staff

The DSL will ensure that all safeguarding training given to staff includes elements of online safety, including how the internet can facilitate abuse and exploitation, and understanding the expectations, roles and responsibilities relating to filtering and monitoring systems. All staff will be made aware that pupils are at risk of abuse, by their peers and by adults, online as well as in person, and that, often, abuse will take place concurrently via online channels and in daily life.

## Online safety and the curriculum

Online safety is embedded throughout the curriculum; however, it is particularly addressed in the following subjects:

- Relationships and health education (Ten:Ten)
- PSHE (Ten:Ten)
- Computing (Kapow)

# Online Safety Policy

Online safety teaching is always appropriate to pupils' ages and developmental stages.

Pupils are taught the underpinning knowledge and behaviours that can help them to navigate the online world safely and confidently regardless of the device, platform or app they are using. The underpinning knowledge and behaviours pupils learn through the curriculum include the following:

- How to evaluate what they see online
- How to recognise techniques used for persuasion
- Acceptable and unacceptable online behaviour
- How to identify online risks
- How and when to seek support
- Knowledge and behaviours that are covered in the government's online media literacy strategy

The online risks pupils may face online are always considered when developing the curriculum. The risks that are considered and how they are covered in the curriculum can be found in Appendix B of this policy.

The DSL and relevant members of staff will:

- Be involved with the development of the school's online safety curriculum. Pupils will be consulted on the online safety curriculum, where appropriate, due to their unique knowledge of the kinds of websites they and their peers frequent and the kinds of behaviours in which they engage online
- Work with relevant members of staff, e.g. the SENCO and designated teacher for LAC, to ensure the curriculum is tailored so that pupils who may be more vulnerable to online harms, e.g. pupils with SEND and LAC, receive the information and support they need

The school will also endeavour to take a more personalised or contextualised approach to teaching about online safety for more susceptible children, and in response to instances of harmful online behaviour from pupils.

Class teachers will review external resources prior to using them for the online safety curriculum, to ensure they are appropriate for the cohort of pupils.

External visitors may be invited into school to help with the delivery of certain aspects of the online safety curriculum. The Head and DSL will decide when it is appropriate to invite external groups into school and ensure the visitors selected are appropriate and quality assured

Before conducting a lesson or activity on online safety, the class teacher and DSL will consider the topic that is being covered and the potential that pupils in the class have suffered or may be suffering from online abuse or harm in this way. The DSL will advise the staff member on how to best support any pupil who may be especially impacted by a lesson or activity. Lessons and activities will be planned carefully so they do not draw attention to a pupil who is being or has been abused or harmed online, to avoid publicising the abuse.

During an online safety lesson or activity, the class teacher will ensure a safe environment is maintained in which pupils feel comfortable to say what they feel and ask questions, and are not worried about getting into trouble or being judged.

If a staff member is concerned about anything pupils raise during online safety lessons and activities, they will make a report in line with the Child Protection and Safeguarding Policy.

If a pupil makes a disclosure to a member of staff regarding online abuse following a lesson or activity, the staff member will follow the reporting procedure outlined in the School's Safeguarding Policy.

# Online Safety Policy

## Use of technology in the classroom

A wide range of technology will be used during lessons, including the following:

- Computers
- Laptops
- Ipads
- Email
- Cameras

Prior to using any websites, tools, apps or other online platforms in the classroom, or recommending that pupils use these platforms at home, the class teacher will review and evaluate the resource. Class teachers will ensure that any internet-derived materials are used in line with copyright law.

Pupils will be supervised when using online materials during lesson time – this supervision is suitable to their age and ability.

## Educating parents

The school will work in partnership with parents to ensure pupils stay safe online at school and at home. Parents will be provided with information about the school's approach to online safety and their role in protecting their children. Parents will be sent a copy of the Acceptable Use Agreement at each academic year and upon any policy review and changes and are encouraged to go through this with their child to ensure their child understands the document and the implications of not following it.

Parents will be made aware of the various ways in which their children may be at risk online, including, but not limited to:

- Child sexual abuse, including grooming
- Exposure to radicalising content
- Sharing of indecent imagery of pupils, e.g. sexting
- Cyberbullying
- Exposure to age-inappropriate content, e.g. pornography
- Exposure to harmful content, e.g. content that encourages self-destructive behaviour.

Parents will be informed of the ways in which they can prevent their child from accessing harmful content at home, e.g. by implementing parental controls to block age-inappropriate content.

Parental awareness regarding how they can support their children to be safe online will be raised in the following ways:

- Parents' evenings
- Social media posts
- Monthly newsletters
- Links to online resources

Parents can access further information about the following topics via safeguarding page on the school website

- Digital wellbeing
- Gaming
- Screen time
- Online bullying / cyber bullying
- AI generated images
- Online  harassment
- Parental controls

- Live streaming
- Reporting
- Healthy relationships
- Social media
- Grooming

Parents can also access further information about the following topics and how our school deal with incidents via the policies listed here

- Child-on-child abuse (Child-on-Child Abuse Policy)
- Online hoaxes and harmful online challenges (Safeguarding Policy)
- Cyber bullying (Anti-bullying Policy)
- Grooming and exploitation including child criminal exploitation, child sexual exploitation and radicalisation (Safeguarding Policy)
- Mental health (Safeguarding Policy)

**Childline –** Report Remove Tool
https://www.childline.org.uk/info-advice/bullying-abuse-safety/online-mobile-safety/report-remove/

**National Centre for Missing & Exploited Children –** Take It Down Tool
https://takeitdown.ncmec.org/

## Internet access

Pupils, staff and other members of the school community will only be granted access to the school's internet network once they have read and signed the Acceptable Use Agreement. A record will be kept of users who have been granted internet access within our school or via our school 365 portal at home.

All members of the school community will be encouraged to use the school's internet network, instead of 3G, 4G and 5G networks, as the network has appropriate filtering and monitoring to ensure individuals are using the internet appropriately.

## Filtering and monitoring online activity

Requests regarding making changes to the filtering system:

- Should be directed to the Head or DSL
- Prior to making any changes to the filtering system, DSLs will conduct a risk assessment (in conjunction with the ICT technicians)
- Any changes made to the system will be recorded by ICT technicians
- Reports of inappropriate websites or materials will be made to an ICT technician immediately, who will investigate the matter and make any necessary changes,

Deliberate breaches of the filtering system:

- Must be reported to the DSL and ICT technicians, who will escalate the matter appropriately
- If a pupil has deliberately breached the filtering system, they will be disciplined in line with the Behaviour Policy
- If a member of staff has deliberately breached the filtering system, they will be disciplined in line with the Disciplinary Policy.

If material that is believed to be illegal is accessed, inadvertently or deliberately, this material will be reported to the appropriate agency immediately, e.g. the Internet Watch Foundation (IWF), CEOP and/or the police.

# Online Safety Policy

All users of the network and school-owned devices will be informed about how and why the school-owned devices are monitored. **Concerns identified through monitoring pupil activity must be reported to the DSL who will manage the situation in line with the School's Safeguarding Policy**.

## Network security

Technical security features, such as anti-virus software, will be kept up-to-date and managed by ICT technicians. Firewalls will be switched on at all times. ICT technicians will review the firewalls on a annual basis to ensure they are running correctly, and to carry out any required updates.

They are advised not to open unfamiliar email attachments. ICT technicians will be alerted to malware and virus attacks via a central management console but would expect staff and students to report any suspicious or unusual device behaviour to them ASAP.

All members of staff will have their own unique usernames and private passwords to access the school's systems. Where available pupils in Reception and above will be provided with their own unique username and private passwords. Staff members and pupils will be responsible for keeping their passwords private. Password complexity rules will be applied by the ICT technicians. Passwords for older learners and staff should be generated in accordance with the NCSC's 'Three Random Words' guidance.

Users will inform ICT technicians if they forget their login details, who will arrange for the user to access the systems under different login details. Users will not be permitted to share their login details with others and will not be allowed to log in as another user at any time. If a user is found to be sharing their login details or otherwise mistreating the password system, the OLICAT Head of IT will be informed and will decide the necessary action to take.
Users will be required to lock access to devices and systems when they are not in use.

## Data security: files and Cloud storage

Where available staff are expected to use Microsoft OneDrive / SharePoint for storage of all files and folders. When accessing and storing folders staff must always follow the Data Protection (GDPR) Policy.

## Emails

Access to and the use of emails will be managed in line with the Data Protection (GDPR) Policy, Acceptable Use Agreement.

Staff and pupils will be given approved school email accounts and will only be able to use these accounts at school and when doing school-related work outside of school hours. Prior to being authorised to use the email system, staff and pupils must agree to and sign the Acceptable Use Agreement. Personal email accounts will not be permitted to be used on the school site. Any email that contains sensitive or personal information will only be sent using secure and encrypted email.

Staff members and pupils will be required to block spam and junk mail, and report the matter to ICT technicians. The school's monitoring system can detect inappropriate links, malware and profanity within emails – staff and pupils will be made aware of this. Chain letters, spam and all other emails from unknown sources will be deleted without being opened. The DSL/Online Safety Lead will organise an **annual** assembly where they explain what a phishing email and other malicious emails might look like – this assembly will includes information on the following:

- How to determine whether an email address is legitimate
- The types of address a phishing email could use
- The importance of asking "does the email urge you to act immediately?"
- The importance of checking the spelling and grammar of an email

Any cyber-attacks initiated through emails will be managed in line with the Data Protection (GDPR) Policy and Critical Incident / Emergency Plan.

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

**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/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.

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.

**Examining electronic devices**

The headteacher, and any member of staff authorised to do so by the headteacher and D.S.L staff 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
- 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:

- Make an assessment of 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 / DSL / appropriate staff member]
- 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 staff member in conjunction with the DSL / headteacher / other member of the senior leadership team] 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/carer 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:

- 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 / searches and confiscation 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.

## Generative artificial intelligence (AI)

The school will take steps to prepare pupils for changing and emerging technologies, e.g. generative AI and how to use them safely and appropriately with consideration given to pupils' age.

The school will ensure its IT system includes appropriate filtering and monitoring systems to limit pupil's ability to access or create harmful or inappropriate content through generative AI.

The school will ensure that pupils are not accessing or creating harmful or inappropriate content, including through generative AI.

The school will take steps to ensure that personal and sensitive data is not entered into generative AI tools and that it is not identifiable.

# Online Safety Policy

The school will make use of any guidance and support that enables it to have a safe, secure and reliable foundation in place before using more powerful technology such as generative AI.

## Use of devices including mobile devices and digital images

Staff members and pupils will be issued with school-owned devices to assist with their work, where necessary. Requirements around the use of school-owned devices can be found in the Acceptable Use Agreement and Data Protection (GDPR) Policy.

When taking pupils off site, personal phones or school issued trip phones can, if necessary be used to phone parents/carers/pupils.

Staff should avoid, wherever possible, using their own personal devices to record digital images (photos or videos) of pupils, rather they should be using school owned mobile devices. Where this is not practical, the images should be transferred to the school network shared drives, including school cloud storage (Google Drive), or to an official school social media account (such as a department 'x' account) and then the original photos should be removed from the private phone, and any personal backups deleted. Staff should not store images or videos of pupils on their own personal devices.

Staff will not post images of pupils from other schools on school social media (for example in sports fixtures).

The school record of parental permissions granted/not granted must be adhered to when taking images of the school's pupils. A list will be circulated by the admin team and referred to by staff when taking photos of pupils. It is best practice when posting an image of a child to not associate their name with the photo.

In accordance with the guidance from the Information Commissioner's Office, parents/carers are welcome to take videos and digital images of their children at events for their own personal use. To respect everyone's privacy and in some cases protection, these images should not be published/made publicly available on social networking sites, nor should parents/carers comment on any activities involving other pupils in the digital image(s).

### Use of own equipment

The use of personal devices on the school premises and for the purposes of school work will be managed in line with the Acceptable Use Agreement and Data Protection (GDPR) Policy.

Pupils may to bring their own phones into to school in Year 6 but must hand them into their class teacher at the start of each day and they must not be used in school.

### Use of school equipment

No personally owned applications or software packages should be installed on to school IT equipment.

Personal or sensitive data (belonging to staff) should not be stored on the local drives of desktop or laptop PCs. If it is necessary to do so, the local drive must be encrypted.

All users should ensure any screens are locked (by pressing Windows + L keys together) before moving away from a computer during the normal working day to protect any personal, sensitive, confidential or classified data and to prevent unauthorised access.

## Social media sites

Young people will not be allowed on social media sites from school equipment. Filtering solutions will be in place to not give access to those sites.

Staff users will follow the expectations set out in our HR and safeguarding policies regarding use of social media. Only official school social media accounts should be used to communicate news and events with parents/carers/pupils. If a department social media account is set up, the administration must be shared within a department for the sake of openness and transparency, and admin details shared with the Admin team/head teacher/D.S.L.

Staff users should not reveal names of staff, pupils, parents/carers or any other member of the school community online on any personal social media site.

Parents/carers/pupils should be aware that the school will investigate the misuse of social media if it impacts on the well-being of other pupils or stakeholders. If inappropriate comments are placed on social media sites about the school or school staff, then advice would be sought from the relevant agencies, including the police if necessary.

The school will use social media in positive ways to publicise, inform and communicate information.

## Sharing nudes and semi-nudes

Responding to incidents of sharing nudes and semi-nudes is complex because of its legal status. Making, possessing and distributing any imagery of someone under 18 which is 'indecent' is illegal. This includes imagery of yourself if you are under 18.

The relevant legislation is contained in the Protection of Children Act 1978 (England and Wales) as amended in the Sexual Offences Act 2003 (England and Wales).

Specifically:

- it is an offence to possess, distribute, show and make indecent images of children
- the Sexual Offences Act 2003 (England and Wales) defines a child, for the purposes of indecent images, as anyone under the age of 18

'Indecent' is not defined in legislation. When cases are prosecuted, the question of whether any photograph of a child is indecent is for a jury, magistrate or district judge to decide based on what is the recognised standard of propriety.

Indecent imagery does not always mean nudity; however, images are likely to be defined as such if they meet one or more of the following criteria:

- nude or semi-nude sexual posing (e.g. displaying genitals and/or breasts or overtly sexual images of young people in their underwear)
- someone nude or semi-nude touching themselves in a sexual way
- any sexual activity involving a child
- someone hurting someone else sexually
- sexual activity that includes animals

The non-consensual sharing of private sexual images or videos with the intent to cause distress is also illegal. The relevant legislation is contained in section 33 of the Criminal Justice and Courts Act 2015.

Many professionals may refer to 'nudes and semi-nudes' as:

- youth produced sexual imagery or 'youth involved' sexual imagery

- indecent imagery - this is the legal term used to define nude or semi-nude images and videos of children and young people under the age of 18
- 'sexting' - many adults may use this term, however some young people interpret sexting as 'writing and sharing explicit messages with people they know' rather than sharing images
- image-based sexual abuse - this term may be used when referring to the non-consensual sharing of nudes and semi-nudes.

These laws weren't created to criminalise young people but to protect them.

Although sharing sexual images of themselves is illegal and risky, it is often the result of curiosity and exploration. Young people need education, support, and safeguarding, not criminalisation. Government guidance on sharing nudes and semi-nudes (updated March 2024) will be followed.

The school will look to support pupils that choose to undertake this risky activity with assemblies, whole class and individual teaching and outside agency referrals where appropriate. The school will try, where possible, to resolve such issues without involving the police. However, in some circumstances, the police must always be involved.

**Handling incidents**

- refer to the Designated Safeguarding Lead (DSL)
- DSL or member of safeguarding team will meet with the young people involved
- staff will not view the image unless it is unavoidable (see section below titled 'viewing images')
- safeguarding staff will take appropriate steps to discuss with parents/carers
- if there is any concern that the young person is at risk of harm, social care or the police to be contacted

Staff will always refer to the police or social care if incident involves:

- an adult
- coercion, blackmail, or grooming
- concerns about capacity to consent
- malicious intent (the non-consensual sharing of private sexual images or videos with the intent to cause distress is also illegal - the relevant legislation is contained in section 33 of the Criminal Justice and Courts Act 2015)
- images show atypical sexual behaviour for the child's developmental stage
- violent acts are depicted
- image shows sex acts and includes a child under 13
- a young person at risk of immediate harm as a result of the disclosure (for example, self-harm or suicide)
- persistent behaviour

**Viewing images**

- staff should avoid viewing indecent images, instead, respond to what you have been told the image contains
- if it is felt necessary to view, discuss with the Head or DSL first
- staff should never copy, print, or share the image (it's illegal)
  if it is felt necessary to view the image, members of the safeguarding team should view with another member of safeguarding team present
- staff will record the fact that the images were viewed in writing to the D.S.L (following our safeguarding procedures) along with reasons and who was present.

**Deleting images (from devices and social media)**

If the DSL has decided that involving other agencies is not necessary, consideration should be given to deleting the images.

Pupils will be asked to delete the images themselves and confirm they have done so. This should be recorded, signed, and dated and passed on to The D.S.L in line with our safeguarding policy.

Any refusal to delete the images should be treated seriously, reminding the pupil that possession is unlawful. Parents will be informed.

## Financially motivated incidents – 'sextortion'

Financially motivated sexual extortion (often known as 'sextortion') is an adult-involved incident in which an adult offender (or offenders) threatens to release nudes or semi-nudes of a child or young person unless they pay money or do something else to benefit them.

Unlike other adult-involved incidents, financially motivated sexual extortion is usually carried out by offenders working in sophisticated organised crime groups (OCGs) overseas and are only motivated by profit. Adults are usually targeted by these groups too.

Offenders will often use a false identity, sometimes posing as a child or young person, or hack another young person's account to make initial contact. To financially blackmail the child or young person, they may:

- groom or coerce the child or young person into sending nudes or semi-nudes and financially blackmail them
- use images that have been stolen from the child or young person taken through hacking their account
- use digitally manipulated images, including AI-generated images, of the child or young person

The offender may demand payment or the use of the victim's bank account for the purposes of money laundering.

Signs to be aware of:

Potential signs of adult-involved financially motivated sexual extortion can include the child or young person being:

- contacted by an online account that they do not know but appears to be another child or young person. They may be contacted by a hacked account of a child or young person
- quickly engaged in sexually explicit communications which may include the offender sharing an image first
- moved from a public to a private/E2EE platform
- pressured into taking nudes or semi-nudes
- told they have been hacked and they have access to their images, personal information and contacts
- blackmailed into sending money or sharing bank account details after sharing an image or the offender sharing hacked or digitally manipulated images of the child or young person

Further information on 'sextortion' can be found here:

- National Crime Agency – www.nationalcrimeagency.gov.uk/what-we-do/crime-threats/kidnap-and-extortion/sextortion-webcam-blackmail
- Internet Watch Foundation – www.iwf.org.uk/resources/sextortion

## Remote learning

All remote learning will be delivered in line with the school policy. This policy specifically sets out how online safety will be considered when delivering remote education.

## Monitoring and review

The DSL, in conjunction with the Head, will monitor the effectiveness of this policy in line with their individual monitoring strategy – see Appendix C.

The school recognises that the online world is constantly changing; therefore, the DSL, ICT technicians and the Head conduct annually light-touch reviews of this policy.

The trust board will ensure that this policy is reviewed annually by the central team, DSLs and IT provider, and following any online safety incidents.

**Appendix A – Pupil Acceptable Use Agreement**

# *St. Brendan's Catholic Primary School*

# *Acceptable Use Policy*

Approved Date: Spring 2026

Review Date: Spring 2027

*'Always treat others as you would like them to treat you.'*

# St Brendan's Catholic Primary School Staff Acceptable Use Policy 2026-2027

**Introduction**

Digital technologies are central to the education, wellbeing and daily lives of children, young people and adults. They provide powerful tools for learning, creativity, communication and collaboration. With these opportunities come responsibilities. All users must understand how to use technology safely, respectfully and lawfully.

This Acceptable Use Policy ensures that:

- staff and volunteers use digital technologies safely, responsibly and professionally.
- school systems, data and users are protected from accidental or deliberate misuse.
- safeguarding, data protection and online safety expectations are met in line with statutory guidance.
- pupils receive high-quality education in digital literacy and online safety

This policy aligns with **Keeping Children Safe in Education (KCSIE 2025/26)**, the **Online Safety Act 2023**, the **Data Protection Act 2018**, **UK GDPR**, and current **Ofsted expectations** for online safety.

All staff and volunteers are expected to read, understand and follow this policy.

# Staff (and Volunteer) Acceptable Use Policy Agreement – Updated for 2026

I understand that I must use school systems in a safe, responsible and professional manner, ensuring that my actions do not put myself, pupils, colleagues or the school at risk. I recognise the importance of modelling safe and respectful online behaviour and embedding online safety within my work with pupils.

**1. Professional and Personal Safety**

- I understand that St Brendan's Catholic Primary School monitors and logs the use of all digital systems, including internet use, email, cloud platforms, and school devices.
- I understand that this policy applies to use of school systems both **on and off site**, and to the use of **personal devices** when used for school purposes.

- I will keep my passwords secure and will not share them with anyone. I will not store passwords in an insecure manner.
- I will report any safeguarding concern, online safety incident, cyber-security risk, or exposure to illegal/inappropriate content immediately to the Designated Safeguarding Lead (DSL) or appropriate senior staff member.
- I will not use digital technologies in any way that could compromise my professional reputation or the reputation of the school.

**2. Professional Conduct and Communication**

- I will communicate with pupils, parents and colleagues using **only official school systems** (school email, school-approved platforms).
- I will ensure all communication is professional, respectful and appropriate.
- I will not use personal social media, messaging apps or personal email to communicate with pupils or parents.
- I will not post or share anything online that could bring the school into disrepute or breach confidentiality.
- I will follow the school's policy on digital/video images and will only take or use images using **school-approved devices**, unless explicit permission has been granted.
- I will ensure that images of pupils are used in line with parental consent and never identify pupils by full name.

**3. Use of Devices and School Systems**

- I will ensure that any personal device used for school purposes (e.g., accessing email, planning, remote learning) is password-protected, kept secure, and has up-to-date security software.
- I will not install unauthorised software or attempt to alter system settings.
- I will not attempt to bypass or disable filtering, monitoring or security systems.
- I will not engage in large downloads, streaming or activities that could disrupt school network performance.
- I will immediately report any damage, malfunction or security concern involving school equipment or software.

**4. Data Protection and Information Security**

- I will follow the school's Data Protection Policy and understand my responsibilities under **UK GDPR** and the **Data Protection Act 2018**.
- I will ensure that personal data is accessed only when necessary, kept secure, and shared only with authorised individuals.
- I will use encrypted methods when transferring digital personal data outside the school network.
- I will ensure that paper-based confidential information is stored securely in locked storage.

- I will not store school data on unapproved devices or cloud services.
- I will report any data breach or suspected breach immediately.

**5. Safe and Legal Use of Online Content**

- I will not access, download, upload or share illegal or inappropriate material, including extremist content, pornography, hate material or content harmful to children.
- I will respect copyright and licensing laws and will not use or distribute copyrighted materials without permission.
- I will ensure that any online content I use for teaching is age-appropriate and safe for pupils.

**6. Use of Artificial Intelligence (AI) and Emerging Technologies (2026 Requirement)**

- I will use AI tools only in line with school policy and will not input personal data, pupil work, or confidential information into external AI systems.
- I will ensure that any AI-generated content used for teaching is checked for accuracy, appropriateness and bias.
- I will not use AI tools to make decisions about pupils or staff.
- I will model safe and ethical use of AI for pupils.

**7. Remote Learning and Online Teaching**

- I will follow school procedures for remote learning, including safeguarding expectations.
- I will ensure that online sessions are conducted through approved platforms and follow school guidance on professional conduct, background settings, and recording.
- I will not conduct one-to-one online sessions with pupils unless authorised and risk-assessed.

**8. Responsibilities and Consequences**

- I understand that this policy applies to my use of school systems **in and out of school**, and to my use of personal devices when used for school-related activities.
- I understand that breaches of this policy may result in disciplinary action, including referral to governors, the Local Authority, or external agencies.
- I understand that illegal activity may result in police involvement.

**Staff / Volunteer Declaration**

I have read and understood the Acceptable Use Policy (2026) and agree to use school digital technology systems and personal devices (when used for school purposes) in accordance with these guidelines.

**Name:**_____

**Signature:** _____

**Date:** _____

## Acceptable Use Agreement for Community Users

Community users are expected to use school systems, networks and devices in a safe, responsible and lawful manner. This agreement applies to all use of school equipment and to any personal devices brought onto the school site.

By using school systems, I agree to the following:

**Safe and Responsible Use**

- I understand that all use of school systems, devices, internet access and digital communications may be monitored and logged for safeguarding, security and compliance purposes.
- I will use any personal device brought into school in a manner that is appropriate for a primary school environment and in line with school policies.
- I will not attempt to access, upload, download or share any illegal, harmful or inappropriate material. This includes material that is abusive, extremist, discriminatory, pornographic, or otherwise unsuitable for a school setting.
- I will not attempt to bypass or interfere with the school's filtering, monitoring or security systems.

**Reporting and Safeguarding**

- I will immediately report any illegal, inappropriate, harmful or concerning content, behaviour or incident to a member of school staff.
- I understand that safeguarding and the protection of children is a priority, and I will act in accordance with school safeguarding procedures.

**Respect for Others and Their Work**

- I will not access, copy, delete, alter or share another user's files or information without permission.
- I will only take or publish images of others with their explicit permission and in line with the school's policies.
- I will not use personal devices to record images or videos unless permission has been granted by the school.
- If images are published, I will ensure that individuals cannot be identified by name or through personal information.

**Use of Information and Online Behaviour**

- I will not publish, post or share any information obtained within the school on personal websites, social media or other online platforms without the school's permission.
- I will not engage in online behaviour that could cause harm, distress or reputational damage to the school or its community.

- I will not make large downloads or uploads that could disrupt the school's network without permission.

**Security and Equipment**

- I will not install software, applications or programmes on school devices, nor attempt to alter system settings, unless authorised.
- I will not damage, disable or tamper with school equipment or the equipment of others.
- I will immediately report any damage, faults or security concerns involving equipment, devices or software.

**Copyright and Intellectual Property**

- I will ensure that I have permission to use the original work of others.
- I will respect copyright and licensing laws and will not download, copy or distribute copyrighted materials (including music, videos or software) without permission.

**Consequences of Misuse**

- I understand that failure to follow this Acceptable Use Agreement may result in the withdrawal of access to school systems and devices.
- Serious or repeated breaches may result in further action in line with school policies and relevant legislation.

**Declaration**

I have read and understood this Acceptable Use Agreement and agree to use school digital technology systems and my own devices (when used on school premises or for school-related purposes) in accordance with these guidelines.

**Name:** _____

**Signed:** _____

**Date:** _____

# Acceptable Use Agreement for Younger Pupils (Foundation Stage / KS1)

**How we stay safe when we use computers, tablets and the internet**

When I use computers, tablets or other technology at school:

- I will **ask a teacher or trusted adult** if I want to use a computer or tablet.
- I will **only use the apps, games or websites** that a teacher or trusted adult has said I can use.
- I will **take care** of the computer, tablet and other equipment.
- I will **ask for help** if I am not sure what to do or if something goes wrong.
- I will **tell a teacher or trusted adult straight away** if I see something that makes me feel worried, sad or confused.
- I know that if I do not follow these rules, I might not be allowed to use the computer or tablet

These rules help keep me safe when I am learning and playing online.

**Signed (child):** _____

**Signed (parent / carer):** _____

**Date:** _____

# Online Safety Policy

## SEND Pupil Acceptable Use Agreement (Parent/Carer-Signed )

**For pupils who need support to understand or follow online-safety rules**

Some children need help to understand how to use technology safely. This agreement is for parents and carers to sign on behalf of their child. It explains how the school will support your child and what we ask from families to help keep them safe.

**How we help your child stay safe when using technology**

When your child uses computers, tablets or other digital devices in school:

- A trusted adult will always supervise and support them.
- Staff will choose safe, appropriate apps, games and websites for your child to use.
- Staff will help your child learn simple rules about staying safe online, at a level that suits their needs.
- Staff will help your child if they are unsure, make a mistake, or see something that worries them.
- Staff will report and respond to any online-safety concerns in line with safeguarding procedures.

**What we ask from parents and carers**

By signing this agreement, you confirm that:

- You understand that your child may need extra support to use technology safely.
- You give permission for your child to use school devices under supervision.
- You understand that the school uses filtering, monitoring and safeguarding systems to help keep children safe online.
- You will speak to school staff if you have any concerns about your child's online behaviour or anything they may have seen.
- You will support the school's online-safety approach at home, as far as is appropriate for your child's needs.

**Use of images and digital work**

- The school will only take or use photos/videos of your child in line with your consent choices.
- Images will never be used in a way that identifies your child by full name.
- You can change your consent at any time by contacting the school office.

**If your child struggles with the rules**

We understand that some children with SEND may find it difficult to follow online-safety rules. If this happens:

- staff will support and teach your child in a positive, appropriate way
- we may adjust access to technology to keep them safe

- we will always work with you to find the best approach for your child

**Parent/Carer Declaration**

I have read and understood this agreement. I understand that the school will support my child to use technology safely and that I can speak to staff at any time if I have concerns.

**Child's Name:** _____

**Parent/Carer Name:** _____

**Signature:** _____

**Date:** _____

# Online Safety Policy

## KS2 Pupil Acceptable Use Agreement

I understand that I must use school computers, tablets, the internet and other digital tools safely and responsibly. These rules help keep me and others safe.

**Keeping Myself Safe Online**

- I know that the school checks how I use computers, devices and the internet to help keep everyone safe.
- I will keep my username and password private and will not share them with anyone.
- I will not use anyone else's username or password.
- I will not share personal information about myself or others online (such as full name, address, school name, phone number, photos, or passwords).
- I will be careful when talking to people online and remember that not everyone is who they say they are.
- If I ever see something online that worries, upsets or confuses me, I will tell a trusted adult straight away.
- I will never arrange to meet someone I have spoken to online without checking with a trusted adult first.

**Using Technology Responsibly**

- I understand that school devices and the internet are for learning. I will only use them for other things if a teacher gives me permission.
- I will not try to download or upload large files unless I have permission.
- I will not use school devices for online gaming, gambling, shopping, file-sharing or video streaming unless a teacher has said I can.
- I will not try to access or search for anything that is rude, dangerous, illegal or inappropriate.

**Respecting Others**

- I will respect other people's work and will not look at, change or delete their files without permission.
- I will be kind, polite and responsible when I communicate online.
- I will not use unkind, rude, aggressive or inappropriate language.
- I understand that cyber-bullying is not acceptable and will be treated seriously.
- I will not take photos or videos of anyone without their permission, and I will not share images without checking with a teacher.

**Keeping School Systems Safe**

- I will only bring my own devices (such as USB sticks) into school if I have permission.

# Online Safety Policy

- If I use my own device in school, I will follow the same rules as when using school equipment.
- I will not try to bypass or disable the school's filtering or security systems.
- I will not install software, apps or programmes on school devices.
- I will not open email attachments or links unless I am sure they are safe and from someone I trust.
- I will tell a teacher straight away if something is broken, not working properly or if I think there may be a problem with the computer or network.

**Using Information and Online Content**

- I will check that information I find online is reliable, as not everything on the internet is true.
- I will not copy someone else's work and pretend it is my own.
- I will follow copyright rules and will not download music, videos or other content that I do not have permission to use.

**My Behaviour In and Out of School**

- I understand that these rules apply when I am using school devices **and** when my behaviour outside school affects the school community.
- This includes things like cyber-bullying, sharing images, or posting unkind or unsafe messages.
- I understand that breaking these rules may lead to consequences such as losing access to school devices, contacting parents, or other actions in line with school behaviour and safeguarding policies.

**Pupil and Parent/Carer Agreement**

By signing below, we confirm that we have read and understood this Acceptable Use Agreement and agree to follow the rules.

**Pupil Name:** _____

**Pupil Signature:** _____

**Parent/Carer Name:** _____

**Parent/Carer Signature:** _____

**Date:** _____

# Online Safety Policy

## KS2 Pupil Acceptable Use Agreement

I understand that I must use school computers, tablets, the internet and other digital tools safely, respectfully and responsibly. These rules help keep me and others safe.

**1. Keeping Myself Safe Online**

- I know that the school monitors how I use computers, devices and the internet to help keep everyone safe.
- I will keep my username and password private and will not share them with anyone.
- I will not use anyone else's username or password.
- I will not share personal information about myself or others online (such as full name, address, phone number, school name, photos, passwords or any private details).
- I will be careful when talking to people online and remember that not everyone is who they say they are.
- I will never arrange to meet someone I have spoken to online without checking with a trusted adult first.
- If I see anything online that worries, upsets or confuses me, I will tell a trusted adult straight away.

**2. Using Technology Responsibly**

- I understand that school devices and the internet are for learning. I will only use them for other things if a teacher gives me permission.
- I will not try to download or upload large files unless I have permission.
- I will not use school devices for online gaming, gambling, shopping, file-sharing or video streaming unless a teacher has said I can.
- I will not try to access or search for anything that is rude, dangerous, illegal or inappropriate.

**3. Respecting Others**

- I will respect other people's work and will not look at, change or delete their files without permission.
- I will be kind, polite and responsible when I communicate online.
- I will not use unkind, rude, aggressive or inappropriate language.
- I understand that cyber-bullying is not acceptable and will be treated seriously.
- I will not take photos or videos of anyone without their permission, and I will not share images without checking with a teacher.

# Online Safety Policy

### 4. Keeping School Systems Safe

- I will only bring my own devices (such as USB sticks) into school if I have permission.
- If I use my own device in school, I will follow the same rules as when using school equipment.
- I will not try to bypass or disable the school's filtering or security systems.
- I will not install software, apps or programmes on school devices.
- I will not open email attachments or links unless I am sure they are safe and from someone I trust.
- I will tell a teacher straight away if something is broken, not working properly or if I think there may be a problem with the computer or network.

### 5. Using Information and Online Content

- I will check that information I find online is reliable, because not everything on the internet is true.
- I will not copy someone else's work and pretend it is my own.
- I will follow copyright rules and will not download music, videos or other content that I do not have permission to use.

### 6. My Behaviour In and Out of School

- I understand that these rules apply when I am using school devices **and** when my behaviour outside school affects the school community.
- This includes things like cyber-bullying, sharing images, or posting unkind or unsafe messages.
- I understand that breaking these rules may lead to consequences such as losing access to school devices, contacting parents, or other actions in line with school behaviour and safeguarding policies.

## KS2 Pupil Acceptable Use Agreement Form

This form relates to the KS2 Acceptable Use Agreement. Please complete the sections below to show that you have read, understood and agree to follow the rules.

I agree to follow these guidelines when:

- I use school systems and devices (in school and at home).
- I use my own devices in school (when allowed).
- I use my own equipment outside school in a way that is linked to school (for example, communicating with classmates, using school email, or accessing school platforms).

**Name of Student / Pupil:** _____

**Group / Class:** _____

**Pupil Signature:** _____

**Date:** _____

# Online Safety Policy

## Parent / Carer Acceptable Use Agreement 2026-2027

Digital technologies are an essential part of children's lives, both in school and at home. They provide powerful opportunities for learning, creativity, communication and collaboration. With these opportunities come responsibilities. Children and young people must be supported to use technology safely, respectfully and responsibly.

This Acceptable Use Agreement is designed to ensure that:

- children use the internet and digital technologies safely for learning, communication and recreation
- school systems, data and users are protected from accidental or deliberate misuse
- parents and carers understand the importance of online safety and work in partnership with the school to support safe online behaviour

The school aims to provide pupils with safe, secure and high-quality access to digital technologies to enhance their learning. In return, pupils are expected to follow the rules set out in the Student Acceptable Use Agreement. A copy of this agreement is attached so that parents and carers are fully aware of the expectations for their child.

Parents and carers are asked to sign the permission form below to show their support for the school's online-safety approach and their commitment to working with the school to keep children safe online.

# Online Safety Policy

## Parent / Carer Permission Form

**Parent / Carer Name:** _____

**Student / Pupil Name:** _____

As the parent/carer of the above pupil:

- I give permission for my child to access the internet and use ICT systems, devices and digital technologies at school.
- I understand that the school has discussed the Acceptable Use Agreement with my child and that they receive (or will receive) age-appropriate online-safety education to help them understand how to use technology safely, both in and out of school.
- I understand that my child may be asked to sign their own Acceptable Use Agreement.
- I understand that the school uses a range of safety measures—including filtering, monitoring and safeguarding systems—to help protect pupils when using school devices and networks.
- I understand that, although the school takes all reasonable precautions, it cannot be held responsible for the content accessed on the internet outside its control.
- I understand that my child's activity on school systems may be monitored and that the school will contact me if they have concerns about any breaches of the Acceptable Use Agreement.
- I will support the school's approach to online safety and encourage my child to use the internet and digital technologies safely and responsibly at home.
- I will contact the school if I have any concerns about my child's online behaviour or safety.

**Signed:** _____

**Date:** _____

# Online Safety Policy

## Appendix B – Online Harm and Risks – Curriculum Coverage

| Subject area | Description and teaching content | Curriculum area the harm or risk is covered in |
|---|---|---|
| **How to navigate the internet and manage information** | | |
| Age restrictions | Some online activities have age restrictions because they include content which is not appropriate for children under a specific age. Teaching will include the following:<br>• That age verification exists and why some online platforms ask users to verify their age<br>• Why age restrictions exist<br>• That content that requires age verification can be damaging to under-age consumers<br>• What the age of digital consent is (13 for most platforms) and why it is important | This risk or harm will be covered in the following curriculum areas:<br>• PSHE<br>• Computing |
| How content can be used and shared | Knowing what happens to information, comments or images that are put online. Teaching will include the following:<br>• What a digital footprint is, how it develops and how it can affect pupils' futures<br>• How cookies work<br>• How content can be shared, tagged and traced<br>• How difficult it is to remove something once it has been shared online<br>• What is illegal online, e.g. youth-produced sexual imagery (sexting) | This risk or harm will be covered in the following curriculum areas:<br>• PSHE<br>• Computing |
| Disinformation, misinformation and hoaxes | Some information shared online is accidentally or intentionally wrong, misleading or exaggerated. Teaching will include the following:<br>• Disinformation and why individuals or groups choose to share false information in order to deliberately deceive<br>• Misinformation and being aware that false and misleading information can be shared inadvertently<br>• Misinformation and understanding that some genuine information can be published with the deliberate intent to harm, e.g. releasing private information or photographs<br>• Online hoaxes, which can be deliberately and inadvertently spread for a variety of reasons<br>• That the widespread nature of this sort of content can often appear to be a stamp of authenticity, making it important to evaluate what is seen online<br>• How to measure and check authenticity online<br>• The potential consequences of sharing information that may not be true | This risk or harm will be covered in the following curriculum areas:<br>• PSHE<br>• Computing |
| Fake websites and scam emails | Fake websites and scam emails are used to extort data, money, images and other things that can either be used by the scammer to harm the person targeted or sold on for financial, or other, gain. Teaching will include the following: | This risk or harm will be covered in the following curriculum areas: |

| | | |
|---|---|---|
| | • How to recognise fake URLs and websites<br>• What secure markings on websites are and how to assess the sources of emails<br>• The risks of entering information to a website which is not secure<br>• What pupils should do if they are harmed, targeted, or groomed as a result of interacting with a fake website or scam email<br>• Who pupils should go to for support<br>• The risk of 'too good to be true' online offers, advertising and fake product sales designed to persuade people to part with money for products and services that do not exist | • PSHE<br>• Computing |
| Online fraud | Fraud can take place online and can have serious consequences for individuals and organisations. Teaching will include the following:<br>• What identity fraud, scams and phishing are<br>• That online fraud can be highly sophisticated and that anyone can be a victim<br>• How to protect yourself and others against different types of online fraud<br>• How to identify 'money mule' schemes and recruiters<br>• The risk of online social engineering to facilitate authorised push payment fraud, where a victim is tricked into sending a payment to the criminal<br>• The risk of sharing personal information that could be used by fraudsters<br>• That children are sometimes targeted to access adults' data<br>• What 'good' companies will and will not do when it comes to personal details<br>• How to report fraud, phishing attempts, suspicious websites and adverts | This risk or harm will be covered in the following curriculum areas:<br>• PSHE<br>• Computing |
| Password phishing | Password phishing is the process by which people try to find out individuals' passwords so they can access protected content. Teaching will include the following:<br>• Why passwords are important, how to keep them safe and that others might try to get people to reveal them<br>• How to recognise phishing scams<br>• The importance of online security to protect against viruses that are designed to gain access to password information<br>• What to do when a password is compromised or thought to be compromised | This risk or harm will be covered in the following curriculum areas:<br>• Relationships education<br>• Computing |
| Personal data | Online platforms and search engines gather personal data – this is often referred to as 'harvesting' or 'farming'. Teaching will include the following:<br>• How cookies work<br>• How data is farmed from sources which look neutral<br>• How and why personal data is shared by online companies<br>• How pupils can protect themselves and that acting quickly is essential when something happens<br>• The rights children have with regards to their data<br>• How to limit the data companies can gather | This risk or harm will be covered in the following curriculum areas:<br>• PSHE<br>• Computing |

| | | |
|---|---|---|
| Persuasive design | Many devices, apps and games are designed to keep users online for longer than they might have planned or desired. Teaching will include the following:<br>• That the majority of games and platforms are designed to make money, and that their primary driver is to encourage people to stay online for as long as possible to encourage them to spend money or generate advertising revenue<br>• How notifications are used to pull users back online | This risk or harm will be covered in the following curriculum areas:<br>• PSHE<br>• Computing |
| Privacy settings | Almost all devices, websites, apps and other online services come with privacy settings that can be used to control what is shared. Teaching will include the following:<br>• How to find information about privacy settings on various sites, apps, devices and platforms<br>• That privacy settings have limitations | This risk or harm will be covered in the following curriculum areas:<br>• PSHE<br>• Computing |
| Targeting of online content | Much of the information seen online is a result of some form of targeting. Teaching will include the following:<br>• How adverts seen at the top of online searches and social media have often come from companies paying to be on there and different people will see different adverts<br>• How the targeting is done<br>• The concept of clickbait and how companies can use it to draw people to their sites and services | This risk or harm will be covered in the following curriculum areas:<br>• PSHE<br>• Computing |
| **How to stay safe online** | | |
| Online abuse | Some online behaviours are abusive. They are negative in nature, potentially harmful and, in some cases, can be illegal. Teaching will include the following:<br>• The types of online abuse, including sexual harassment, bullying, trolling and intimidation<br>• When online abuse can become illegal<br>• How to respond to online abuse and how to access support<br>• How to respond when the abuse is anonymous<br>• The potential implications of online abuse<br>• What acceptable and unacceptable online behaviours look like | This risk or harm will be covered in the following curriculum areas:<br>• PSHE<br>• Computing |
| Radicalisation | Pupils are at risk of accessing inappropriate and harmful extremist content online, including terrorist material. Extremist and terrorist groups use social media to identify and target vulnerable individuals. Teaching will include the following:<br>• How to recognise extremist behaviour and content online<br>• Which actions could be identified as criminal activity<br>• Techniques used for persuasion<br>• How to access support from trusted individuals and organisations | All areas of the curriculum |
| Challenges | Online challenges acquire mass followings and encourage others to take part in what they suggest. Teaching will include the following:<br>• What an online challenge is and that, while some will be fun and harmless, others may be dangerous and even illegal<br>• How to assess if the challenge is safe or potentially harmful, including considering who has generated the challenge and why | This risk or harm will be covered in the following curriculum areas:<br>• PSHE |

| | | |
|---|---|---|
| | • That it is okay to say no and to not take part in a challenge<br>• How and where to go for help<br>• The importance of telling an adult about challenges which include threats or secrecy, such as 'chain letter' style challenges | • Computing<br>Relationships education |
| Fake profiles | Not everyone online is who they say they are. Teaching will include the following:<br>• That, in some cases, profiles may be people posing as someone they are not or may be 'bots'<br>• How to look out for fake profiles | This risk or harm will be covered in the following curriculum areas:<br>• PSHE<br>• Computing |
| Grooming | Knowing about the different types of grooming and motivations for it, e.g. radicalisation, child sexual abuse and exploitation, gangs and financial exploitation. Teaching will include the following:<br>• Boundaries in friendships with peers, in families, and with others<br>• Key indicators of grooming behaviour<br>• The importance of disengaging from contact with suspected grooming and telling a trusted adult<br>• How and where to report grooming both in school and to the police<br>At all stages, it is important to balance teaching pupils about making sensible decisions to stay safe whilst being clear it is never the fault of the child who is abused and why victim blaming is always wrong. | This risk or harm will be covered in the following curriculum areas:<br>• PSHE<br>• Computing |
| Livestreaming | Livestreaming (showing a video of yourself in real-time online, either privately or to a public audience) can be popular with children, but it carries a risk when carrying out and watching it. Teaching will include the following:<br>• What the risks of carrying out livestreaming are, e.g. the potential for people to record livestreams and share the content<br>• That online behaviours should mirror offline behaviours and that this should be considered when making a livestream<br>• That pupils should not feel pressured to do something online that they would not do offline<br>• The risk of watching videos that are being livestreamed, e.g. there is no way of knowing what will be shown next<br>• The risks of grooming | This risk or harm will be covered in the following curriculum areas:<br>• PSHE<br>• Computing |
| Pornography | Knowing that sexually explicit material presents a distorted picture of sexual behaviours. Teaching will include the following:<br>• That pornography is not an accurate portrayal of adult sexual relationships<br>• That viewing pornography can lead to skewed beliefs about sex and, in some circumstances, can normalise violent sexual behaviour<br>• That not all people featured in pornographic material are doing so willingly, e.g. revenge porn or people trafficked into sex work | This risk or harm will be covered in the following curriculum areas:<br>Not covered in primary school. |

| | | |
|---|---|---|
| Unsafe communication | Knowing different strategies for staying safe when communicating with others, especially people they do not know or have not met. Teaching will include the following:<br>• That communicating safely online and protecting your privacy and data is important, regardless of who you are communicating with<br>• How to identify indicators of risk and unsafe communications<br>• The risks associated with giving out addresses, phone numbers or email addresses to people pupils do not know, or arranging to meet someone they have not met before<br>• What online consent is and how to develop strategies to confidently say no to both friends and strangers online | This risk or harm will be covered in the following curriculum areas:<br>• PSHE<br>• Computing |
| **Wellbeing** | | |
| Impact on confidence (including body confidence) | Knowing about the impact of comparisons to 'unrealistic' online images. Teaching will include the following:<br>• The issue of using image filters and digital enhancement<br>• The role of social media influencers, including that they are paid to influence the behaviour of their followers<br>• That 'easy money' lifestyles and offers may be too good to be true<br>• The issue of photo manipulation, including why people do it and how to look out for it | This risk or harm will be covered in the following curriculum areas:<br>• PSHE<br>• Computing |
| Impact on quality of life, physical and mental health and relationships | Knowing how to identify when online behaviours stop being fun and begin to create anxiety, including that there needs to be a balance between time spent online and offline. Teaching will include the following:<br>• How to evaluate critically what pupils are doing online, why they are doing it and for how long (screen time)<br>• How to consider quality vs. quantity of online activity<br>• The need for pupils to consider if they are actually enjoying being online or just doing it out of habit, due to peer pressure or due to the fear or missing out<br>• That time spent online gives users less time to do other activities, which can lead some users to become physically inactive<br>• The impact that excessive social media usage can have on levels of anxiety, depression and other mental health issues<br>• That isolation and loneliness can affect pupils and that it is very important for them to discuss their feelings with an adult and seek support<br>• Where to get help | This risk or harm will be covered in the following curriculum areas:<br>• PSHE<br>• Computing |
| Online vs. offline behaviours | People can often behave differently online to how they would act face to face. Teaching will include the following:<br>• How and why people can often portray an exaggerated picture of their lives (especially online) and how that can lead to pressure How and why people are unkind or hurtful online when they would not necessarily be unkind to someone face to face | This risk or harm will be covered in the following curriculum areas:<br>• PSHE<br>• Computing |

| | | |
|---|---|---|
| Reputational damage | What users post can affect future career opportunities and relationships – both positively and negatively. Teaching will include the following:<br>• Strategies for positive use<br>• How to build a professional online profile | This risk or harm will be covered in the following curriculum areas:<br>• PSHE<br>• Computing |
| Suicide, self-harm and eating disorders | Pupils may raise topics including eating disorders, self-harm and suicide. Teachers must be aware of the risks of encouraging or making these seem a more viable option for pupils and should take care to avoid giving instructions or methods and avoid using language, videos and images. | • PSHE |

## Appendix C – School Monitoring Strategy

This Section may need to be mapped out still?