PYRFORD CHURCH OF ENGLAND PRIMARY SCHOOL

ONLINE SAFETY POLICY

Approval Date: March 2026

Review Date: Spring 2027

1. Introduction

Online safety is an essential element of safeguarding. It is embedded within the school's safeguarding culture and is the responsibility of the entire school community. All staff maintain the attitude that "it could happen here" and are vigilant in recognising and responding to online risks faced by pupils.

Technology is used in every classroom and innovative use of new technologies has the capacity to inspire and scaffold learning, motivate learners and create opportunities to support and challenge at all levels. However, technology must be used safely, securely and responsibly to protect all members of our community. The measures and procedures detailed within this policy allow children and adults to use, learn through, and enjoy technology in a safe environment.

This online safety policy covers the use of all technology which can access the school network and the internet or which facilitates electronic communication from school to beyond the bounds of the school site. This includes but is not limited to desktop computers, laptops, mobile phones, tablets and chrome books. This policy recognises that there are differences between the use of technology as a private individual and as a member of staff / pupil.

The online safety policy should be read alongside those for relationships education, personal electronic devices, data protection, social media, behaviour, child protection and safeguarding, anti-bullying and SEND.

2. Aims

Our school aims to:

- Have robust processes in place to ensure the online safety of pupils, staff, volunteers and governors
- Deliver an effective approach to online safety, which empowers us to protect and educate the whole school community in its use of technology, including mobile and smart technology
- Establish clear mechanisms to identify, intervene and escalate an incident, where appropriate

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

- **Content** – being exposed to illegal, inappropriate or harmful content, such as pornography, fake news, racism, misogyny, self-harm, suicide, antisemitism, radicalisation and extremism
- **Contact** – being subjected to harmful online interaction with other users, such as peer-to-peer pressure, commercial advertising and adults posing as children or young adults with the intention to groom or exploit them for sexual, criminal, financial or other purposes
- **Conduct** – personal online behaviour that increases the likelihood of, or causes, harm, such as making, sending and receiving explicit images (e.g. consensual and non-consensual sharing of nudes and semi-nudes and/or pornography), sharing other explicit images and online bullying; and
- **Commerce** – risks such as online gambling, inappropriate advertising, phishing and/or financial scams

3. Legislation & Guidance

This online safety policy is based on the Department for Education's (DfE's) statutory safeguarding guidance, Keeping Children Safe in Education 2025, and its advice for schools on:

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

This online safety policy 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 also takes into account the National Curriculum computing programmes of study.

4. Using this policy

This online safety policy has been written by the school, building on best practice and government guidance. It has been agreed by senior management and approved by governors. The school's governing body has overall responsibility for monitoring this policy and holding the Headteacher to account for its implementation. The Headteacher is responsible for ensuring that staff understand this policy, and that it is being implemented consistently throughout the school.

The Designated Safeguarding Lead responsible for online safety is: **Louise Vymetal.**

The DSL will:

- Support the Headteacher in ensuring that staff understand this policy and that it is being implemented consistently throughout the school
- Work with the Headteacher, ICT manager and other staff, as necessary, to address any online safety issues or incidents
- Ensure online safety training is provided for staff
- Work with external agencies where appropriate
- Monitor online safety incident logs (including cyber bullying) and ensure they are dealt with appropriately in line with this policy

All staff, visitors and volunteers who are accessing the school's internet are responsible for ensuring that they are implementing the provisions of this policy consistently and understand safeguarding concerns related to online risks. Staff receive online safety training during induction and regular safeguarding updates.

Parents and carers are encouraged to support their children's safe use of technology at home. The school will provide guidance and updates to parents through a range of means including: the school website; newsletters; school communications; training and surveys.

5. Managing Online Access

The school will provide managed internet access to its staff and pupils in order to help pupils to learn how to assess and manage risk, to gain the knowledge and understanding to keep themselves safe when using the internet and to bridge the gap between school IT systems and the more open systems outside the school.

- The school will use a recognised internet service provider or regional broadband consortium.
- The school will ensure that all internet access has age appropriate filtering provided by a recognised filtering system which is regularly checked to ensure that it is working, effective and reasonable.
- The school will ensure that its networks have virus and anti-spam protection.
- Access to school networks will be controlled by personal passwords.
- Systems will be in place to ensure that internet use can be monitored and a log of any incidents will be kept to help to identify patterns of behaviour and to inform online safety policy.
- The security of school IT systems will be reviewed regularly.
- All staff that manage filtering systems or monitor IT use will be supervised by senior management and have clear procedures for reporting issues.
- The school will ensure that access to the internet via school equipment for anyone not employed by the school is filtered and monitored.

6. Internet Use

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.

Communication with Pupils and Families

All communication between staff and pupils or families must take place using school-approved systems including: school email; Seesaw and ScoPay. Staff must not communicate with pupils through personal email accounts, social media or messaging apps.

Email

- Staff may only use approved email accounts on the school IT systems.
- Staff to parent email communication must only take place via a school email address or from within the learning platform.
- Incoming email should be treated as suspicious and attachments not opened unless the author is known.

Published content (e.g. school website, school social media accounts)

- The contact details will be the school address, email and telephone number. Staff or pupils' personal information will not be published.
- The Headteacher or nominee will take overall editorial responsibility and ensure that content is accurate and appropriate.

Publishing Pupils' Images and Work

Written parental consent will be obtained before images or names of pupils are published online. Parents are reminded that content shared via Seesaw must not be downloaded or shared outside the platform.

Use of social media

The school has a separate social media policy. Pupils do not have access to social networking sites in school. Pupils are taught about the risks of social media use and their digital footprint as part of the computing curriculum.

Staff and pupils should ensure that their online activity, both in school and out takes into account the feelings of others and is appropriate for their situation as a member of the school community. Where inappropriate use occurs, swift action will be taken in line with the social media policy.

Use of personal devices

Personal equipment may be used by staff to access the school IT systems provided their use complies with the provisions of this policy. Staff must not take or store images of pupils or pupil personal data on personal devices. The school cannot be held responsible for the loss or damage of any personal devices used in school or for school business.

The Personal Electronic Devices Policy provides guidance for pupil use of personal devices.

Protecting personal data

The school has a separate Data Handling Policy. It covers the use of biometrics in school, access to pupil and staff personal data on and off site, remote access to school systems.

Acceptable internet use for pupils

Pupils are taught about acceptable use of the internet both in school and outside (see section 6 below). When using the school's ICT systems, pupils are required to:

- Ask an adult before accessing the internet
- Only use websites that an adult authorised them to use and only use school devices for school work
- Only use the magic badge and Scratch username and password they have been given and never share any personal information
- Look after the school's ICT equipment and tell an adult if something is broken or not working properly
- Tell an adult immediately if any online issues arise

Guidelines for acceptable internet use are discussed with children and displayed in classrooms.

7. Online Safety Education

Pupils are taught about online safety in a number of ways:

- Online safety topics are comprehensively taught through the computing curriculum in line with Government guidance. Online safety is taught discretely in every year group at the beginning of each year, with key messages reinforced throughout the year
- Online safety topics are included with the PSHE curriculum and lessons

- Assemblies and bespoke lessons are used to provide education about specific issues and themes, including for Safer Internet Day
- Pupil surveys are conducted led by pupil Digital Leaders with results shared and discussed in classes

Pupils are taught about:

- Online identity and self-image – Understand that online actions and profiles shape how others see them; begin to reflect on their own digital identity.
- Online relationships and communication – Learn how to communicate safely and respectfully online; recognise appropriate vs. inappropriate interactions.
- Online reputation and digital footprint – Introduce the idea that things shared online can last and affect themselves or others.
- Managing online content and information – Begin to evaluate information they see online, recognise obvious false content, and understand age-appropriate sources.
- Recognising risks and online harm – Identify common online risks (e.g., bullying, scams, inappropriate content) and know who to ask for help.
- Privacy, security, and responsible use – Learn basic online safety habits: protecting passwords, keeping personal information private, and respecting digital content rules.
- Healthy use of technology – Understand balance in screen time, and that technology can have positive and negative effects on wellbeing.

Online safety education for pupils is underpinned by the core idea of communication, with the key message of "Tell a trusted adult" for any issues experienced online.

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

8. Cyberbullying

To help prevent cyber-bullying, we will ensure that pupils understand what it is and what to do if they become aware of it happening to them or others. We will ensure that pupils know how they can report any incidents and are encouraged to do so, including where they are a witness rather than the victim.

The school will actively discuss cyber-bullying with pupils, explaining the reasons why it occurs, the forms it may take and what the consequences can be. Class teachers will discuss cyber-bullying with their class.

Cyberbullying can include, but is not limited to, the following:

- Threatening, intimidating or upsetting text messages
- Threatening or embarrassing pictures and video clips sent via mobile phone cameras
- Silent or abusive phone calls or using the victim's phone to harass others, to make them think the victim is responsible
- Threatening or bullying emails, possibly sent using a pseudonym or someone else's name
- Unpleasant messages sent via instant messaging
- Unpleasant or defamatory information posted to blogs, personal websites and social networking sites, e.g. Facebook

- Abuse between young people in intimate relationships online i.e. teenage relationship abuse
- Discriminatory bullying online i.e. homophobia, racism, misogyny/misandry.

The school will be aware that certain pupils can be more at risk of abuse and/or bullying online, such as LGBTQ+ pupils and pupils with SEND.

Cyberbullying against pupils or staff is not tolerated under any circumstances. Incidents of cyberbullying are dealt with quickly and effectively wherever they occur in line with the Anti-bullying Policy.

9. Policy Decisions

Authorising access

- All staff receive information on Acceptable Use / ICT Code of Conduct in the Employee Handbook before accessing the school IT systems.
- At EYFS & Key Stage 1, access to the internet will be by adult demonstration with supervised access to specific, approved online material.
- At Key Stage 2, access to the internet will be with teacher permission with increasing levels of autonomy.

Assessing risks

- The school will take all reasonable precautions to prevent access to inappropriate material. However, due to the international scale and linked internet content, it is not possible to guarantee that unsuitable material will never appear on a school computer. The school cannot accept liability for the material accessed, or any consequences of internet access.

Handling online safety complaints and concerns

- Complaints or concerns of internet misuse, including cyber-bullying, will be dealt with according to the school behaviour policy.
- Complaints or concerns of a child protection nature must be dealt with in accordance with safeguarding / child protection procedures, set out in the Child Protection & Safeguarding Policy.
- Pupils and parents will be informed of consequences and sanctions for pupils misusing the internet and this will be in line with the school's behaviour policy.

10. Communication of the Policy

To pupils

- Online safety is taught through the computing and PSHE curriculum and through wider safeguarding education. Pupils are made aware of the acceptable use of ICT equipment and the internet at school.

To staff

- All staff will be shown where to access the online safety policy and its importance explained.
- All staff receive a copy of the Employee Handbook which details use of the school IT systems and use of internet whilst on school premises.
- All staff will receive online safety training as part of the safeguarding training.

To parents

- The school make all new parents aware of how to use the internet acceptably as part of the admissions process when they register their child with the school. They are asked to agree to the acceptable use policy provided by the school.
- Parents' and carers' attention will be drawn to the school online safety policy in newsletters and on the school website.
- Parents and carers are given updates on online safety issues, when necessary, via the school newsletter, training and other means.

11. Monitoring and Review

This policy will be reviewed regularly by the Senior Leadership Team and governing body. The review will consider:

- emerging online risks
- incident logs
- changes to safeguarding guidance
- updates to DfE online safety expectations.