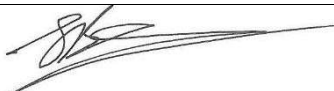


<b>Name of Policy</b>	<b>Online Safety Policy</b>
<b>School Lead</b>	School E-Safety Officer
<b>Date of Approval</b>	02.10.25
<b>Date of next Review</b>	October 2026
<b>Links to other policies</b>	<ul style="list-style-type: none"> <li>- Child Protection and Safeguarding Policy.</li> <li>- Procedures for responding to concerns about a child or young person's wellbeing.</li> <li>- Dealing with allegations of abuse made against a child or young person.</li> <li>- Managing allegations against staff and volunteers.</li> <li>- Code of conduct for staff and volunteers.</li> <li>- Anti-bullying policy and procedures.</li> <li>- ICT Acceptable Use Policy.</li> <li>- Prevent Risk Assessment and Action Plan.</li> <li>- Remote Learning Policy</li> </ul>
<b>Head teacher sign off signature and date</b>	 02.10.25

## ➤ Contents

- Purpose.

- Legal framework.
- Aims.
- Categories of risk.
- Online abuse
- Filtering and Monitoring
- Generated Artificial Intelligence
- Social Media
- Online Bullying (Cyberbullying)
- Pilgrim Discord Platform
- Remote Learning
- How we keep young people safe
- Pupil Learning
- Related policies and procedures.
- Contact details.
- This policy should be read alongside The Pilgrim School's policies and procedures on child protection and safeguarding.
- [Visit the NSPCC website for more safeguarding and child protection information.](#)

## ➤ Purpose

At The Pilgrim School, we work closely with children, young people, and their families as part of our core educational mission and wider school activities.

This policy is designed to:

- Prioritise the safety, welfare, and wellbeing of children and young people when they access or interact with the internet, social media, and mobile technology.
- Provide clear principles and guidance for staff and volunteers to support a consistent and responsible approach to online safety.
- Ensure that the school's use of digital technology aligns with our core values and complies with all relevant legal and statutory requirements.

This policy applies to all staff, volunteers, pupils, and anyone participating in or connected to activities carried out by The Pilgrim School.

## ➤ Legal framework

This Online Safety Policy has been developed in accordance with current legislation, statutory guidance, and best practice aimed at safeguarding children in England. It reflects key national documents and guidance that support the protection and wellbeing of pupils in an online context.

The policy draws on and aligns with:

- **Teaching Online Safety in Schools (2023)**  
[View the guidance](#)
- **Harmful Online Challenges and Online Hoaxes (2021)**  
[View the guidance](#)
- **Meeting Digital and Technology Standards in Schools and Colleges: Filtering and Monitoring (2025)**  
<https://www.gov.uk/guidance/meeting-digital-and-technology-standards-in-schools-and-colleges/filtering-and-monitoring-standards-for-schools-and-colleges>
- **Generative AI: Product Safety Expectations (2025)**  
<https://www.gov.uk/government/publications/generative-ai-product-safety-expectations/generative-ai-product-safety-expectations>
- **Keeping Children Safe in Education (2025)**  
This statutory guidance sets out the legal duties schools must follow to safeguard and promote the welfare of children.  
<https://www.gov.uk/government/publications/keeping-children-safe-in-education--2>

Additionally, summaries of key legislation and guidance relating to:

- **Online Abuse**
- **Bullying**
- **Child Protection**

...can be accessed through the NSPCC: NSPCC Online Safety Resources

<https://www.nspcc.org.uk/keeping-children-safe/online-safety/>

## ➤ **Aims**

At Pilgrim School, we are committed to creating a safe and supportive environment for all members of our community. We believe:

- No one should ever experience abuse of any kind. While we acknowledge the reality that abuse can and does happen, we are proactive in our efforts to prevent it.
- Everyone—especially children and young people—should be able to access the internet safely for learning and personal development. Appropriate safeguards must be in place to ensure their safety at all times.

We recognise that:

- The online world offers immense opportunities for education, connection, and creativity. However, it also presents significant risks and challenges.

- We have a duty of care to protect all individuals involved in our school community from potential harm online.
- As educators, we carry a special responsibility to safeguard children and young people in the digital environment—both when they are using The Pilgrim School’s networks and devices, and when accessing the internet remotely or at home.
- Collaborating with children, young people, parents, carers, and external agencies is vital in promoting digital wellbeing and supporting responsible online behaviour.
- Given that many of our pupils may be accessing learning remotely, we must continually adapt our practices to promote safe online access at home.
- Every individual, regardless of age, disability, gender identity, race, religion or belief, sex, or sexual orientation, has the right to equal protection from all forms of harm and abuse.

We are committed to inclusive safeguarding practices that take into account the specific needs and experiences of:

- Find out more about:
  - Safeguarding children who come from Black, Asian and minoritised ethnic communities.
  - Safeguarding d/Deaf and disabled children and young people.
  - Safeguarding LGBTQ+ children and young people.
  - Safeguarding children with special educational needs and disabilities (SEND).

## ➤ Categories of Risk

Safeguarding children from harmful and inappropriate online content is a fundamental responsibility of all schools and colleges. A strong, whole-school approach to online safety enables the school community—including pupils and staff—to use technology safely and responsibly. It also ensures that effective systems are in place to identify, address, and escalate any concerns when needed.

Online safety is a broad and constantly evolving area. Risks can be grouped into four main categories:

### **1. Content**

Exposure to inappropriate, harmful, or illegal material, such as:

- Pornography
- Misinformation, Disinformation (including fake news) and Conspiracy Theories
- Racism and misogyny
- Content promoting self-harm or suicide
- Anti-Semitic material
- Radicalisation and extremist content

## 2. Contact

Harmful interactions with others online, including:

- Peer pressure and coercion
- Manipulative or targeted advertising
- Adults posing as children or young people with intent to groom or exploit for sexual, criminal, financial, or other purposes

## 3. Conduct

Behaviours online that can cause harm or increase the risk of harm, such as:

- Creating, sending, or receiving explicit images (including consensual and non-consensual sharing of nudes or pornography)
- Sharing harmful or explicit content
- Cyberbullying and harassment

## 4. Commerce

Risks related to online financial safety, including:

- Gambling sites and apps
- Inappropriate or misleading advertising
- Phishing attempts and online scams

If you believe a pupil, Pupil, or member of staff may be at risk, please report your concerns immediately to the DSL and by contacting: [support@lcsit.com](mailto:support@lcsit.com).

### ➤ **Online Abuse**

- At The Pilgrim School, we take online abuse very seriously and are committed to responding promptly and effectively. Our approach includes:
- **Clear safeguarding procedures:** We have comprehensive safeguarding and child protection policies that outline how we respond to all forms of abuse, including online abuse. These procedures ensure a consistent and robust response.
- **Access to expert support:** For additional guidance and assistance, we liaise with the Professional Online Safety Helpline. They can be contacted at 0344 381 4772 or [helpline@saferinternet.org.uk](mailto:helpline@saferinternet.org.uk).

- **Staff and volunteer training:** All staff and volunteers receive regular training to identify and manage all types of abuse—such as bullying, cyberbullying, emotional abuse, sexting, sexual abuse and exploitation, radicalisation, extremism, and other harmful online challenges or hoaxes.
- **Holistic support:** Our response considers the needs of those experiencing abuse, any witnesses, and the wider school community to ensure appropriate care and safeguarding.
- **Ongoing review:** We regularly review and update our action plans addressing online abuse to ensure issues are resolved sustainably and effectively.
- **Clear points of contact:** Each pupil has multiple designated contacts within the school, including the Designated Safeguarding Lead and Deputy. Staff and pupils are directed to these contacts as well as to the Lincolnshire Local Authority Designated Officers and Lincolnshire County Council's Safeguarding in Schools team. Staff receive safeguarding training appropriate to their roles, and the Online Safety Officer can refer any concerns to the Professional Online Safety Helpline via the UK Safer Internet Centre.

### ➤ Filtering and Monitoring

Schools and colleges have a legal duty to safeguard Pupils both online and offline. Governing bodies must ensure that effective **filtering** and **monitoring** systems are in place, in line with statutory guidance such as *Keeping Children Safe in Education* and the *Prevent Duty*.

- **Filtering** is a preventative measure that blocks access to illegal, inappropriate, or harmful content (e.g., certain websites, images, videos).
- **Monitoring** is reactive and tracks user activity to identify potential risks, such as exposure to harmful content or signs of bullying. This can be done manually or through software that generates alerts based on concerning behaviour.

While no system is foolproof, schools must:

- Understand the **capabilities and limitations** of their filtering system.
- **Mitigate risks** where gaps exist.
- Ensure systems do not **unreasonably hinder teaching, learning, or digital literacy**, allowing pupils to learn how to manage online risks responsibly.

These tools support safeguarding responsibilities and require collaboration between leadership, safeguarding leads, and IT staff.

At the Pilgrim school, our Filtering and Monitoring reports are provided weekly by LCS and reviewed and actioned by the Online Safety Officer and DSL.

## ➤ Generated Artificial Intelligence (AI)

Generative AI is a type of **artificial intelligence** that can **create new content** — such as text, images, music, or even videos — by learning from examples. At Pilgrim we want to outline the acceptable use of Generative Artificial Intelligence (AI) tools —such as ChatGPT, DALL·E, Copilot, and other text, image, code, or audio generators—by Pupils and staff within the educational environment. The goal is to promote responsible, ethical, and informed use of these technologies to enhance learning, creativity, and critical thinking.

### 1. Acceptable Use

Generative AI may be used for educational purposes under the following conditions:

- **Learning Support:** Pupils may use AI tools for idea generation, study assistance, or to clarify complex topics, provided the tool is used as a supplement, not a substitute, for learning.
- **Creative Projects:** AI-generated content may be incorporated into creative assignments (e.g., art, writing, music) if explicitly permitted by the teacher.
- **Coding Assistance:** Pupils may use AI for code examples or debugging support, but must understand and be able to explain the submitted work.
- **Teacher Use:** Educators may use AI tools for lesson planning, resource creation, and feedback generation, provided human oversight remains primary.

### 2. Prohibited Use

Pupils and staff must not use Generative AI in ways that:

- **Constitute Academic Dishonesty**, including submitting AI-generated work as wholly original without acknowledgment.
- **Bypass Learning Objectives**, such as using AI to complete tests, quizzes, or assignments meant to assess individual understanding.
- **Produce Harmful Content**, including misinformation, discriminatory, or offensive materials.
- **Infringe Copyright or Privacy**, including generating content based on real individuals without consent or misusing copyrighted material.

### 3. Attribution and Transparency

When Generative AI is used in submitted work, it must be:

- **Clearly Acknowledged**, including what tool was used and how it contributed.
- **Supported by Pupil Understanding**, meaning pupils must be able to discuss and defend any AI-assisted content submitted for assessment.

#### 4. Consequences of Misuse

Improper use of Generative AI will be treated as a breach of the school's ICT Acceptable use policy and code of conduct:

- Warnings, grade penalties, or redoing of assignments.
- Disciplinary action as outlined in the school's code of conduct.

#### ➤ Social Media

##### **Responsible Use of Social Media**

All members of the school community are expected to use social media responsibly and in accordance with this policy. Social media platforms include, but are not limited to, Facebook, Instagram, Twitter (X), TikTok, Snapchat, LinkedIn, YouTube, and messaging apps such as WhatsApp and Discord.

Users must:

- Always communicate respectfully and thoughtfully online.
- Protect their own privacy and the privacy of others by not sharing personal information without consent.
- Avoid posting content that may be harmful, offensive, defamatory, or discriminatory.
- Never represent the school without permission or misrepresent their identity or affiliation.

Staff and pupils should be aware that their online activity, even when conducted outside of the school setting, may impact the wider community and be subject to investigation if it violates this policy. Improper use on social media may be treated as a breach to this policy and the Code of Conduct.

#### ➤ Online Bullying (Cyberbullying)

Online bullying, also known as cyberbullying, involves the use of digital technology to harass, threaten, or humiliate others. It is taken seriously and will not be tolerated under any circumstances.

Examples of online bullying include:

- Sending threatening or abusive messages.
- Spreading rumors or false information.
- Sharing embarrassing or private images or videos without consent.
- Creating fake profiles to harass others.



- Repeatedly excluding someone from online groups or activities.

Anyone who experiences or witnesses online bullying is strongly encouraged to report it immediately to the Designated Safeguarding Lead or an appropriate authority. All reports will be handled promptly and confidentially, with appropriate support provided to those affected.

In line with our Behaviour Policy and the school's disciplinary procedures, action may be taken against individuals found to be engaging in online bullying. Where necessary, incidents will also be referred to the police or relevant external safeguarding agencies.

At Pilgrim, our primary focus is on education and support. In the first instance—and depending on the severity of the incident—we aim to address behaviour through guidance rather than immediate discipline. However, if the behaviour persists or is serious in nature, formal disciplinary measures will be implemented in accordance with our policy.

### ➤ Pilgrim Discord Platform

Pilgrim School has established an official Discord Channel to provide a safe, supportive online space for our pupils to connect, reduce feelings of isolation, and enhance community engagement. This initiative supports our commitment to the wellbeing and digital safety of all pupils.

#### **Access and Eligibility**

- Access to the Pilgrim School Discord Channel is restricted to current pupils using their official Pilgrim School email addresses to ensure a secure and private environment.
- Access will be revoked once pupils complete Year 11 or transition to another educational setting. Future consideration may be given to creating an alumni channel.

#### **Monitoring and Reporting**

- The channel is monitored by designated Pilgrim School staff; however, supervision is not constant. Pupils and parents are encouraged to report any concerns directly to the child's allocated Pastoral Support Worker (PSWS) for timely review and intervention.

#### **Access Hours**

- The channel is available from 8:00 AM to 9:00 PM daily to promote healthy online habits and ensure balanced routines.

#### **Parental Responsibility**

- Pilgrim School's monitoring is limited to the official Discord Channel. Interactions outside this space, including private messages or external channels, fall under parental supervision. Parents and carers are encouraged to actively support and supervise their child's online activities beyond the school-managed environment.

#### **Joining Procedure**

- Pupils wishing to join must scan the provided QR code and register using their Pilgrim School email. Access requests will be reviewed by staff to maintain the channel's safety and integrity.

By participating in the Pilgrim School Discord Channel, pupils and parents agree to adhere to these guidelines, ensuring a positive, respectful, and secure online community.

## **Remote Learning**

This section outlines the expectations and safeguarding measures in place to ensure the safety, privacy, and wellbeing of pupils and staff during remote learning activities.

### **1. Safeguarding During Remote Learning**

- All remote learning must follow the school's safeguarding policies. Staff must remain alert to signs of abuse or distress and report concerns following the school's standard safeguarding procedures.
- Live lessons must only take place on school-approved platforms that are secure and compliant with data protection laws (e.g., Microsoft Teams).
- Staff must conduct live sessions in a professional setting, and where possible, against a neutral background. Pupils should also be encouraged to participate in a safe and appropriate environment.

### **2. Expectations for Pupils**

- Pupils must access remote learning using their school-provided or approved accounts.
- Pupils are expected to behave online in accordance with the school's Behaviour Policy. This includes appropriate communication in chats, respectful engagement during lessons, and not recording or distributing any part of a lesson without permission.
- Pupils should not share meeting links or passwords with others.
- Cameras and microphones should be used appropriately. Pupils may be asked to turn cameras on for registration or engagement purposes, unless they have a valid reason not to (e.g., safeguarding, privacy concerns).
- Pupils must dress appropriately and have a responsible adult present while participating in online lessons.

### **3. Expectations for Staff**

- Staff must use school accounts and devices for remote teaching and communication.
- Lessons should be recorded where appropriate to provide access for absent pupils and for safeguarding purposes, in accordance with the school's data protection policies.
- One-to-one teaching or support should only be conducted with prior approval from a line manager and must be logged. Another adult should be aware the lesson is taking place.

#### 4. Parental Involvement

- Parents/carers are encouraged to support pupils in maintaining safe online practices and ensuring they have a suitable workspace at home.
- The school will provide guidance to parents on how to support safe online learning, including using parental controls and monitoring engagement.

#### 5. Reporting and Responding to Concerns

- Any incidents of inappropriate behaviour or breaches of the Online Safety Policy during remote learning must be reported immediately to the Designated Safeguarding Lead (DSL).
- The school will take appropriate action in line with its Behaviour and Safeguarding Policies, which may include restricting access to online learning or further disciplinary steps.

#### 6. Training and Awareness

- All staff will receive regular training on online safety, including specific guidance for remote learning.
- Pupils will be educated on how to stay safe online as part of the curriculum, including their rights, responsibilities, and how to seek help if needed.

### ➤ [How we keep young people safe](#)

At The Pilgrim School, the safety and wellbeing of our children and young people — both online and offline — is a top priority. We are committed to promoting the responsible, respectful, and secure use of technology for all members of our school community.

We strive to keep children and young people safe online by:

- **Appointing a designated Online Safety Coordinator**, currently Mel Findon, to lead and oversee our online safety strategy.
- **Ensuring all staff complete online safety training** within their first year of employment at Pilgrim.
- **Providing clear guidance** to staff and volunteers on appropriate online conduct, including expectations and professional boundaries when engaging with vulnerable pupils and their families.
- **Empowering pupils** to use the internet, social media, and mobile devices responsibly, safely, and respectfully.
- **Fostering strong, trusting relationships** with pupils so they feel confident to raise concerns and seek help.

- **Encouraging all pupils and visitors** to use the Pilgrim Guest Wi-Fi to help restrict access to appropriate and filtered websites.
- **Engaging and supporting parents and carers** in keeping their children safe online through regular communication, training, and shared resources.
- **Creating an Online Safety Agreement**, developed in collaboration with young people and their parents or carers, to set clear expectations for online behaviour.
- **Offering training and resources** for parents and carers through our website and the *Reach More Parents* app to enhance their digital awareness and confidence.
- **Establishing clear procedures** to respond appropriately to any incidents of online misconduct or harmful behaviour—whether by a child, young person, or adult.
- **Regularly reviewing and updating** the security of our information systems to ensure they are robust and resilient.
- **Effectively managing usernames, logins, passwords, and email accounts** to maintain system security.
- **Monitoring and filtering access** to websites and social media platforms for both pupils and staff, using weekly reports provided by LCS (our dedicated IT safety partner).
- **Protecting personal information** of staff, volunteers, pupils, and families by storing data securely and sharing it only when appropriate.
- **Obtaining written consent** before using images of children, young people, or families—and ensuring they are used only for the purposes agreed.
- **Providing supervision, training, and support** to all staff and volunteers to strengthen their understanding of online safety and their role in promoting it.
- **Delivering Pupil education** on online safety through Safer Internet Day activities, external workshops, and through ICT, PSHE, and tutor time—both in school and in the home setting.
- **Holding termly Pupil Forums** to discuss online safety topics, hear Pupil perspectives, and keep up to date with emerging digital trends.
- **Communicating regularly with parents** via newsletters, Parent Forum, and the *Reach More Parents* app to reinforce our collaborative approach to online safety.
- **Risk assessing any new technologies or social media platforms** before they are introduced into the school environment.
- **Implementing a clear Mobile Phone Protocol**, setting realistic expectations to reduce screen time and limit online access during the school day.
- **Modelling responsible digital behaviour** by all staff and adults in the school community.
- **Maintaining a Prevent Risk Assessment and Action Plan** to identify and manage risks related to radicalisation or extremism, with clear preventive measures in place.

- **Responding to concerns promptly**, in line with our safeguarding, child protection, and behaviour policies.

### ➤ Pupil Learning

At Pilgrim pupils learn the importance of staying safe online through PSHE/IT/Tutor Time lessons as well as through external workshops run by the staying safe partnership.

Our online safety curriculum teaches pupils to:

- Show respect in all online interactions, applying the same principles as face-to-face relationships, including resisting pressure to share personal information or images.
- Critically evaluate online relationships and information sources, understanding risks from people they haven't met and recognizing harmful content or contact.
- Understand the minimum age requirements for social media use (13 years) to protect against exposure to inappropriate content and unsafe contacts.
- Exercise caution when sharing personal information online and use privacy and location settings to safeguard their data.
- Recognize that online content can be widely circulated without control, emphasizing the permanence of shared material.
- Identify and respond appropriately to inappropriate or upsetting online content, knowing where to seek support.
- Understand appropriate boundaries in friendships and play, including online interactions.
- Learn about privacy rights and the importance of not keeping unsafe secrets.
- Recognize the difference between safe and unsafe physical and online contact.
- Respond safely to adults they meet, both online and offline, and identify harmful or dangerous relationships.
- Know how to report abuse, online concerns, or feelings of being unsafe, and develop the confidence and vocabulary to seek help.
- Persist in asking for help for themselves or others, and know where to find advice such as from family, school, or trusted sources.

### ➤ Related policies and procedures

- This policy statement should be read alongside our organisational policies and procedures, including:
  - Safeguarding and Child Protection Policy.

- Procedures for responding to concerns about a child or young person's wellbeing.
- Dealing with allegations of abuse made against a child or young person.
- Managing allegations against staff and volunteers.
- Code of conduct for staff and volunteers.
- Anti-bullying policy and procedures.
- ICT Acceptable Use Policy.
- Prevent Risk Assessment and Action Plan.
- Remote learning.
- Find more information about safeguarding children and child protection.

## **Contact details.**

### **Online safety/E-Safety co-ordinator**

Name: Mel Findon

Phone/email: [mel.findon@pilgrim.lincs.sch.uk](mailto:mel.findon@pilgrim.lincs.sch.uk)

### **Designated Safeguarding Lead**

Name: Mel Findon

Phone/email: [mel.findon@pilgrim.lincs.sch.uk](mailto:mel.findon@pilgrim.lincs.sch.uk)

### **Deputy Designated Safeguarding Lead**

Name: Bev Lee

Phone/email: [bev.lee@pilgrim.lincs.sch.uk](mailto:bev.lee@pilgrim.lincs.sch.uk)

### **Deputy Designated Safeguarding Lead (in the absence of Mel and Bev)**

Name: Elena Wilson

Phone/email: [Elena.wilson@pilgrim.lincs.sch.uk](mailto:Elena.wilson@pilgrim.lincs.sch.uk)

### **Professional Online Safety Helpline**

03443814772

[helpline@saferinternet.org.uk](mailto:helpline@saferinternet.org.uk)

<https://saferinternet.org.uk/professionals-online-safety-helpline>

### **NSPCC Helpline**

0808 800 5000

+ **More ways to help you protect children.**



Take our online safety course  
[nspcc.org.uk/kcso](https://nspcc.org.uk/kcso)



Sign up for our weekly current awareness email newsletter  
[nspcc.org.uk/caspar](https://nspcc.org.uk/caspar)



See information and resources for voluntary and community organisations  
[nspcc.org.uk/vcs](https://nspcc.org.uk/vcs)