Plat Douet School
Digital Safeguarding Policy

September 2026

At Plat Douet School every learner is entitled to a curriculum rich and varied, challenging and inspiring, which enables every individual to reach their fullest potential to the highest possible standard and allow all pupils to ‘be the best they can be’.

Plat Douet School

Digital Safeguarding Policy

1. Aims and Purpose

Computing, digital technologies and the internet are essential parts of modern life and play an increasingly important role in education, communication and social interaction. At Plat Douet School, we recognise the significant educational benefits that technology can provide and are committed to ensuring that all pupils can use digital technologies safely, responsibly and confidently.

The purpose of digital technology and internet use within school is to:

- Enhance teaching and learning and raise educational standards.
- Promote pupil engagement, independence and achievement.
- Provide pupils with opportunities to develop the digital skills they need for life and future employment.
- Support effective communication and collaboration.
- Support the professional work of staff.
- Develop pupils' understanding of responsible and ethical digital citizenship.

Digital safeguarding is a shared responsibility. Staff, pupils, parents and carers, the Digital Safeguarding Coordinator, CYPES and other relevant agencies all have a role to play in keeping children and adults safe when using digital technologies.

The school recognises that digital safeguarding extends beyond access to inappropriate online content. It includes issues such as online communication, cyberbullying, privacy and data protection, online relationships, digital wellbeing, inappropriate use of technology, artificial intelligence, image and video sharing, and the impact of online activity on children's physical and emotional wellbeing.

2. Roles and Responsibilities of the School

The school will:

- Appoint a **Digital Safeguarding Coordinator (DSC)** to oversee digital safeguarding across the school and to monitor, review and develop best practice.
- Ensure the DSC acts as the primary point of contact between the school and CYPES in relation to digital safeguarding matters, including requests for changes to web filtering.
- Ensure digital safeguarding remains a high priority for all staff and that staff understand how and when to report concerns or incidents to the DSC.
- Maintain appropriate records of digital safeguarding incidents and concerns. These records will be made available to CYPES or other relevant agencies where required.
- Safeguard the digital wellbeing and professional privacy of staff, including ensuring that personal information and photographs are not published online without appropriate consent.

- Ensure staff are not required to use personal mobile phones to communicate with pupils or parents. A school-owned device will be available where mobile communication is required for school purposes.

- Evaluate and risk-assess new technologies before they are introduced, ensuring that their anticipated educational benefits are balanced against any potential safeguarding, privacy or data protection risks.

- Embed digital safeguarding within the school's wider safeguarding arrangements, including the home-school agreement and Acceptable Use Policies.

- Obtain appropriate parental consent for the use and sharing of pupil photographs and videos on the school website, social media and other approved school platforms.

- Ensure pupils and parents/carers are regularly provided with relevant, age-appropriate and meaningful information about digital safeguarding, including through newsletters, assemblies, lessons, parent sessions and events such as Safer Internet Week.

- Ensure appropriate technical safeguards, including filtering and monitoring systems, are in place and regularly reviewed.

- Ensure staff receive appropriate training and updates relating to digital safeguarding and emerging technologies.

3. Digital Safeguarding Coordinator

The Digital Safeguarding Coordinator will have a clear understanding of the school's safeguarding, child protection, digital safeguarding and data protection policies and procedures.

The DSC will undertake appropriate training and professional development to maintain an up-to-date understanding of current digital safeguarding concerns, emerging technologies and effective practice.

The DSC will work closely with the Designated Safeguarding Lead/Child Protection Officer where a digital safeguarding concern may also constitute a child protection concern.

Where appropriate, child protection concerns will be referred through the school's established safeguarding procedures and to the relevant external agencies.

The DSC will also have sufficient pedagogical understanding to assess the educational benefits of digital technologies alongside their potential safeguarding risks. They will attend relevant training and support sessions to remain informed about emerging concerns and best practice.

The DSC will challenge, support and advise staff in developing their understanding of digital safeguarding and in providing effective digital safeguarding education to pupils.

4. Key Responsibilities of the Digital Safeguarding Coordinator

The Digital Safeguarding Coordinator will:

- Develop, maintain and regularly review the school's Digital Safeguarding Policy, ensuring that it reflects relevant CYPES requirements and the school's own practice.

- Develop appropriate and differentiated **Acceptable Use Policies (AUPs)** for pupils, staff and other users where appropriate.
- Ensure relevant AUPs are communicated to and, where required, agreed by pupils, parents/carers and staff.
- Establish and maintain a **Digital Safeguarding Log** to record digital safeguarding concerns and incidents.
- Review digital safeguarding provision across the school and identify areas for development.
- Use an appropriate self-evaluation and improvement framework, such as the SWGfL *360° Safe* framework, to support annual review and improvement planning.
- Brief staff regularly on emerging digital safeguarding issues, trends and technologies.
- Monitor systems designed to reduce and, where possible, prevent inappropriate behaviour and access to unacceptable content.
- Manage and maintain appropriate user profiles and web-filtering settings to provide suitable levels of protection while allowing appropriate flexibility for teaching and learning.
- Conduct regular testing to ensure that inappropriate or blocked content remains inaccessible.
- Ensure digital safeguarding information and signage is displayed appropriately throughout the school and refreshed regularly.
- Support staff in responding appropriately to digital safeguarding concerns.
- Monitor emerging technologies, including artificial intelligence, and advise the school on their safe and appropriate use.

5. Artificial Intelligence (AI)

Artificial Intelligence is developing rapidly and has the potential to provide significant benefits to teaching, learning and school administration. However, its use also presents safeguarding, privacy, ethical and educational risks.

Plat Douet School will promote the **safe, responsible, ethical and purposeful use of AI**. AI tools must be used in a way that supports the school's safeguarding, data protection and educational requirements.

Staff use of AI

Staff may use approved AI tools where they provide a clear educational or professional benefit. Staff must:

- Follow school guidance regarding approved AI tools and services.
- Never enter confidential, sensitive or personally identifiable information about pupils, families or staff into an AI tool unless the tool has been specifically approved for that purpose and appropriate data protection arrangements are in place.
- Consider the accuracy and reliability of AI-generated information and check important information before using or sharing it.

- Recognise that AI can produce inaccurate, misleading, biased or inappropriate content.
- Maintain professional judgement and remain responsible for any content, resources or decisions produced with the assistance of AI.
- Check AI-generated resources for age appropriateness, accuracy, accessibility and potential safeguarding concerns.
- Be mindful of copyright, intellectual property and the appropriate attribution of sources.
- Not use AI to make significant decisions about pupils without appropriate human oversight and professional judgement.
- Ensure that the use of AI does not replace appropriate professional interaction, teaching or safeguarding processes.

Pupil use of AI

Pupils will be taught about AI as part of the school's Computing and digital safeguarding curriculum. This will include:

- What AI is and how it is used in everyday life.
- The benefits and limitations of AI.
- The possibility of AI generating inaccurate or misleading information.
- The importance of checking information rather than automatically trusting AI-generated responses.
- The responsible and ethical use of AI.
- Privacy and the importance of not sharing personal information with AI systems.
- The risks associated with AI-generated images, videos, audio and other content.
- The potential for AI to be used to create misleading or harmful content, including deepfakes.
- Appropriate use of AI in learning and the importance of pupils' own ideas, creativity and understanding.

Pupils will not be permitted to use AI tools in ways that breach the school's Acceptable Use Policy or that could compromise the privacy, safety or wellbeing of themselves or others.

The school will regularly review its approach to AI as technology, guidance and risks continue to develop.

6. Roles and Responsibilities of All Staff

All staff are expected to:

- Act promptly on all digital safeguarding concerns and follow the school's Digital Safeguarding Policy and safeguarding procedures.

- Immediately follow child protection procedures where a digital safeguarding concern indicates a potential child protection issue.
- Work within the school's digital safeguarding measures and never attempt to bypass, disable or circumvent filtering, monitoring or other security systems.
- Teach and reinforce appropriate aspects of the school's digital safeguarding programme, including age-appropriate online safety and responsible technology use.
- Maintain appropriate professional boundaries when using digital technologies. This includes:
    - Not giving pupils personal mobile telephone numbers or personal contact details.
    - Not allowing pupils to use staff network accounts or log-in details.
    - Not connecting with pupils through personal social media accounts.
    - Using only school-approved platforms and communication channels when communicating with pupils and families.
- Follow data protection requirements and use approved methods of storing and transferring information, including encrypted memory devices where appropriate.
- Ensure school data is only stored, accessed or transferred using authorised systems and locations.
- Behave in a healthy, positive and professional manner when using digital technologies and participating in online activities.
- Seek advice from the Digital Safeguarding Coordinator when unsure about a digital safeguarding issue, emerging technology or appropriate practice.
- Follow the school's guidance when using artificial intelligence and other emerging technologies.
- Sign and comply with the appropriate Acceptable Use Policy and understand the responsibilities associated with it.

7. Roles and Responsibilities of Pupils

Pupils are expected to:

- Use digital technologies responsibly, respectfully and safely.
- Follow the school's Acceptable Use Policy and any instructions provided by staff.
- Treat others with respect when communicating online and never use technology to bully, threaten, embarrass or deliberately upset another person.
- Keep usernames, passwords and other personal information secure.
- Never attempt to bypass school filtering, monitoring or security systems.
- Tell a trusted adult if they encounter something online that makes them feel uncomfortable, worried or unsafe.

- Think carefully before sharing photographs, videos, messages or other content online.
- Respect the privacy and personal information of others.
- Understand that online actions can have real-world consequences.
- Use AI and other digital technologies responsibly and honestly, following school guidance.

8. Roles and Responsibilities of Parents and Carers

Parents and carers have an important role in supporting the school to promote digital safeguarding.

Parents and carers are expected to:

- Support the school in promoting safe, responsible and appropriate use of digital technologies.
- Read, understand and support the school's Acceptable Use Policy and encourage their children to follow it.
- Discuss online safety, responsible technology use and appropriate online behaviour with their children.
- Encourage their children to speak to a trusted adult if they experience something online that makes them feel uncomfortable or unsafe.
- Be aware of the age restrictions and risks associated with online services, games, apps and social media platforms.
- Support the school's approach to the use of photographs and videos of pupils, including providing appropriate consent where requested.
- Contact the school if they have concerns about their child's use of technology or if an online incident may affect their child's wellbeing or safety in school.
- Support the school's approach to the safe and responsible use of artificial intelligence.

9. Review

This policy will be reviewed regularly and updated when necessary to reflect changes in legislation, CYPES guidance, technology, emerging digital safeguarding risks and the school's own practice.

Digital safeguarding is an evolving area. The school will continue to review and develop its approach to ensure that pupils and staff are supported to use technology safely, responsibly and positively.

Subject Leader: Bernard Rebours

Date: September 2026