Local Procedure Title	**E-Safety**
Service	**Unsted Park School**
ACS Policy number and title	**ACS 38 E-Safety**
Local Procedure template reference	**ACS LP 38**
Local Procedure date	7/9/2024
Local Procedure review date	7/9/2025
Local Procedure Author(s)	Jamie Dowsett
Local Procedure Ratification	Checked and Approved by: Shane Kenny

1. Introduction

At Unsted Park School, e-safety is a critical part of our commitment to providing a secure, supportive learning environment. E-safety means equipping children, young people, and staff with the knowledge and tools to use technology responsibly and safely. We actively educate our students and staff on safe technology use, while ensuring that appropriate measures and response mechanisms are in place to address and support any incidents when they arise.

2. Aims

The aim of this policy is to educate our young people about the benefits and risks of using new technology. At Unsted Park School, we are dedicated to providing safeguards and raising awareness among all users, empowering them to manage their online experiences responsibly and safely.

3. SCOPE

The e-safety policy at Unsted Park School addresses the responsible use of our computing systems, equipment, and software both on-site and off-site. This includes the use of Aspris-owned technology outside of school premises, as well as personal technology brought into our settings. Our policy comprehensively covers essential e-safety areas, including social networking, cyber-bullying, data protection, password security, internet filtering, the responsible use of digital and video images, and regulations for mobile and gaming devices.

4. Key responsibilities

Head Teacher / Head of Care: The Head Teacher or Head of Care at Unsted Park School is responsible for ensuring that all staff understand and consistently implement the e-safety policy across the school and care environments. They must also manage and oversee filtering and monitoring systems, addressing any concerns promptly.

Designated Safeguarding Lead (DSL): The DSL takes lead responsibility for online safety at Unsted Park School. Details of the DSL and deputies are outlined in our safeguarding policies (AOP06/ AOP06A/ AOP06B). Key responsibilities include:

- Logging and managing any online safety incidents in accordance with safeguarding policies.
- Addressing incidents of cyber-bullying.
- Liaising with external agencies or services when necessary to ensure comprehensive online safety.

All Staff and Volunteers: All staff, including contractors, agency staff, and volunteers, are expected to:

- Understand and implement the e-safety policy consistently.
- Collaborate with the DSL to ensure that any online safety incidents are properly logged and managed according to policy guidelines.

Parents / Carers: Parents and carers play a vital role in maintaining e-safety. They are encouraged to:

- Inform school staff or the Head Teacher / Head of Care of any e-safety concerns or questions.
- Seek additional online safety guidance from recommended resources, such as:
    - UK Safer Internet Centre – "What are the issues?"
    - Childnet International – "Hot topics" and "Parent factsheet"
    - Disrespect Nobody – "Healthy relationships"

Visitors: All visitors using Unsted Park School's or Aspris's ICT systems or internet are made aware of this policy and are expected to review and follow it. If necessary, they will be asked to formally agree to the terms.

5. E safety risks at Unsted Park school

At Unsted Park School, the primary e-safety risks are carefully managed and fall into several key categories, with a particular focus on emerging threats such as AI-generated fake accounts, as well as traditional risks like online grooming, social media, sexting, and cyberbullying:

- **Content**: Risks related to exposure to inappropriate material, such as online pornography, age-inappropriate games (often with violent and racist language), substance abuse, and harmful lifestyle websites promoting anorexia, self-harm, or suicide. Students are also taught how to critically assess the authenticity of online content. With the rise of AI technology, there is a growing concern over manipulated content such as deepfakes, which can distort images, videos, and other media. Additionally, AI has been used to create **fake accounts** impersonating students or staff on social media platforms, making it harder to distinguish between legitimate and fraudulent profiles. These fake accounts can be used to spread misinformation, harm reputations, or target students for inappropriate contact.

- **Contact**: One of the most pressing risks is **online grooming**, where individuals attempt to form inappropriate relationships with young people through digital platforms. This includes risks related to **social media**, where students may face peer pressure, exposure to harmful content, or unsolicited contact from strangers. The creation of **fake accounts** using AI to impersonate students increases the danger of online grooming, as perpetrators can hide behind these false identities to manipulate or deceive children. The school provides guidance on protecting personal information online and teaches students how to recognise suspicious online behaviour. Additionally, **cyberbullying** is a key concern, with students potentially facing harassment through social media, messaging apps, or online gaming. Fake accounts can exacerbate this risk, as bullies can hide their identity behind fabricated profiles to avoid detection.

- **Conduct**: Risks linked to online behaviour include **sexting**—sending or receiving intimate or inappropriate images, also referred to as SGII (self-generated indecent images). The school educates students about the dangers of sexting, highlighting how these images can be easily shared beyond the intended recipient, leading to serious emotional, social, and legal consequences. Other risks include managing one's **digital footprint** and online reputation, particularly in relation to social media and the impact of AI-generated content that can distort a student's online presence. Privacy concerns, including the disclosure of personal information, are also covered, along with the potential harm of excessive screen time, especially on social media or gaming platforms. Students are also educated about the importance of respecting **copyright** and intellectual property rights when sharing digital content.

Unsted Park School takes these risks seriously and is committed to educating students, staff, and parents about how to recognise, respond to, and prevent these harmful online behaviours. This includes staying vigilant about the use of AI technologies that can create fake accounts or manipulate digital content, ensuring a safe and supportive digital environment for all.

6. REPORTING AND RESPONDING

At Unsted Park School, safeguarding and child protection are of paramount importance, particularly in relation to online safety. Any disclosure related to e-safety will be handled with the same priority as any other safeguarding concern, in line with the school's Safeguarding Policies (AOP06/ AOP06A/ AOP06B).

Unsted Park School ensures the following:

- **Precautions for Online Safety**: The school will take all reasonable steps to ensure online safety for all students and staff but acknowledges that incidents may still occur, both within and outside the school setting.
- **Reporting of Incidents**: All staff members are made aware of the need to report any online safety issues or incidents. Clear reporting routes are in place, aligned with Aspris's safeguarding procedures, and consistent with policies on whistleblowing, complaints, and managing allegations.
- **Timely Response**: Once an incident is reported, it will be addressed as quickly as possible to ensure a swift and appropriate response.
- **Training and Expertise**: The Designated Safeguarding Lead (DSL), Online Safety Lead, and other responsible staff members have the appropriate training and skills to manage online safety risks effectively.
- **Escalating Serious Concerns**: If an incident suggests illegal activity or the potential for serious harm, it will be escalated immediately through Aspris's safeguarding procedures.
- **Concerns Regarding Staff Misuse**: Any concerns about staff misuse of technology or online platforms will be reported to the Headteacher. If the concern involves the Headteacher, it will be referred to the Operations Director.
- **Incident Reporting System (Engage)**: All online safety incidents will be recorded and managed using the **Engage** system, ensuring proper documentation, follow-up, and accountability.
- **Updating Risk Assessments**: Any e-safety concerns or incidents will be incorporated into the child's individual risk assessments. These updates ensure that any online safety risks, vulnerabilities, or new concerns are reflected in the risk management plan and that staff are informed of any changes in the student's online behaviour or needs.

7. Children and young people's own communication devices

To ensure the safety and well-being of all students, the use of personal communication devices, such as mobile phones, is strictly managed.

- **KS2-KS4**: All mobile phones must be handed in to the designated staff at the start of each school day. Phones will be returned to students at the end of the school day to prevent distractions and ensure a focus on learning.
- **KS5**: A strict "no-show" policy is in place, meaning mobile phones must not be visible or in use during school hours unless expressly permitted for educational purposes.
- **Access to School Phones**: If students need to contact parents or guardians during the school day, they can request permission from a teacher to use a school phone. This ensures that communication is appropriately managed, reducing the risk of misuse and ensuring student safety.

- **Access to Emails and Social Media**: Access to social media is blocked during school hours to maintain a safe and focused learning environment, and to protect students from the risks of cyberbullying and inappropriate online content. Students are provided with school email accounts after receiving written permission from their parents or guardians. These emails are monitored and are intended for educational purposes only to ensure safe and responsible use of digital communication.

This procedure is designed to reduce risks related to e-safety, cyberbullying, and safeguarding concerns. By enforcing these measures, we aim to foster a safe learning environment and protect students from potential online harms. Students are encouraged to communicate through official school channels for urgent matters.

8. MONITORING AND REVIEW

This procedure will be reviewed annually, or earlier if necessary, I update in line with national and/or local updates.

9. Section Title

Content

10.

Contents Checklist (Local Services may add additional items – this is a core list)			
Local responsibilities		Risk assessments	
Contact plans		Access to email	
Correspondence		Access to social media	
Access to telephones		Children and young people's own communication devices	
Record keeping		'Local Rules' for safe and sensible communications and social media use	
Monitoring arrangements			

Local Procedure Review History:

Date Reviewed	Reviewer	Summary of revisions