Path4

Online Safety Policy

1. Policy Statement

Path 4 AP is committed to ensuring that all students and staff use technology, including the internet, in a safe and responsible manner. We recognize the potential risks associated with online activities, including exposure to harmful content, cyberbullying, and misuse of personal data. This **Online Safety Policy** sets out the responsibilities and actions required to safeguard the school community when using technology.

This policy is aligned with statutory guidance including **Keeping Children Safe in Education (KCSIE) 2024** and the **UK Data Protection Act 2018 (GDPR)**.

2. Aims and Objectives

The key aims of this policy are to:

- Protect students and staff from online harm and abuse.
- Ensure all students understand the importance of online safety and behave responsibly online.
- Educate staff on their responsibilities in monitoring and supporting students' safe use of technology.
- Establish a framework for managing online incidents, including breaches of security and misuse of technology.

3. Scope

This policy applies to:

- All students and staff of Path 4 AP.
- All online activities carried out using school equipment or during school hours, including on and off the school premises.
- Any personal use of social media or technology by staff or students that could affect the school's reputation or the well-being of students.

4. Roles and Responsibilities

4.1 The Governing Body

- Ensures that appropriate online safety policies are in place and regularly reviewed.
- Monitors the effectiveness of the school's online safety measures.

4.2 The Head of Centre

- Ensures the implementation of the online safety policy and that staff are trained in online safety.
- Leads the response to any online safety incidents in coordination with the **Designated Safeguarding Lead (DSL)**.

4.3 Designated Safeguarding Lead (DSL)

- Acts as the main point of contact for online safety issues and reports.
- Liaises with relevant authorities, including the police, social services, and the Local Authority Designated Officer (LADO), in cases of online safety concerns.
- Provides advice and support to staff, students, and parents on online safety.

4.4 IT Staff

- Implements appropriate technical measures to safeguard the school's IT infrastructure.
- Ensures that filtering and monitoring systems are in place to block and report harmful content.
- Regularly updates and monitors security settings, firewalls, and anti-virus software.

4.5 All Staff

- Familiarize themselves with this policy and promote online safety awareness to students.
- Monitor student use of technology during lessons and report any concerns to the DSL.
- Ensure that all communication with students online is professional and conducted via school-approved channels.

4.6 Students

- Follow the school's online safety rules and understand the consequences of misusing technology.
- Report any online safety concerns to a trusted adult.

4.7 Parents and Guardians

- Support the school's approach to online safety and promote safe internet usage at home.
- Engage in online safety education with their children.

5. Education and Training

5.1 Students

- Path 4 AP integrates online safety into the curriculum to teach students how to stay safe online.
- Age-appropriate lessons will be provided on topics such as responsible internet use, privacy, cyberbullying, and reporting concerns.

5.2 Staff Training

- All staff will receive annual training on online safety, including understanding the risks, identifying signs of online abuse or bullying, and responding to incidents.
- Staff will be trained to teach and model good online safety practices to students.

5.3 Parent Workshops

- The school will offer workshops and guidance to parents who request support to help them understand the risks associated with technology and how to support their children's safe use of the internet at home.

6. Use of Technology

6.1 School Devices and Networks

- All users of school devices and networks are subject to monitoring and filtering to ensure compliance with the school's online safety rules.
- Users must not install unauthorized software or bypass the school's security systems.

6.2 Personal Devices

- Students are allowed to bring personal devices to school only if approved by the Head of Centre.
- Staff must ensure that any personal devices used to access school systems are protected with up-to-date security software and are only used for professional purposes.

6.3 Social Media

- Staff must not communicate with students via personal social media platforms. All online communications should take place through official school channels.
- Students are advised not to share personal details or communicate with strangers via social media.
- Inappropriate use of social media by staff, students, or parents that negatively affects the school or individuals will result in disciplinary action.

7. Managing Online Safety Incidents

7.1 Types of Online Safety Incidents

Incidents can include but are not limited to:

- Access to inappropriate or harmful content.
- Cyberbullying, harassment, or grooming.
- Unauthorized access to or theft of personal information.
- Use of school resources for illegal or harmful activities.

7.2 Reporting

- **Students**: If a student feels unsafe online or witnesses inappropriate online behaviour, they should report it immediately to a teacher, the DSL, or another trusted adult.
- **Staff**: Staff must report any online safety concerns to the DSL immediately. In serious cases, the Head of Centre should also be notified.

7.3 Response to Incidents

- The school will take swift and appropriate action to respond to any online safety concerns, including removing harmful content, safeguarding the child, and reporting the incident to relevant authorities such as the police or social services.
- In cases of illegal activity, the school will preserve evidence and cooperate fully with external agencies.

7.4 Disciplinary Measures

- Violations of the online safety policy will be treated seriously. Consequences may include restrictions on IT use, parental involvement, suspension, or even exclusion for students.
- Staff who breach the policy will be subject to disciplinary action, which may result in termination of employment.

8. Cyberbullying

- Path 4 AP takes a zero-tolerance approach to cyberbullying. Any form of bullying conducted via digital platforms, such as social media, messaging apps, or gaming, will be dealt with in line with the school's **Anti-Bullying Policy**.
- Staff will provide guidance to students on identifying, reporting, and preventing cyberbullying.

9. Filtering and Monitoring

- Path 4 AP uses appropriate filtering and monitoring systems to prevent access to harmful or inappropriate content. These systems are regularly reviewed to ensure they meet the school's safeguarding needs.
- Staff are responsible for monitoring student use of school devices and internet access during lessons, ensuring that students use technology safely and responsibly.

10. Data Protection and Privacy

- All personal data, including images, video, and communications, will be processed in accordance with the **UK Data Protection Act 2018 (GDPR)**.
- Students and staff will be advised on the importance of protecting personal information and their right to privacy.
- Staff must ensure that any personal data, including images and videos, collected as part of school activities are handled securely and used appropriately.

11. Review and Monitoring

This policy will be reviewed annually by the school's Senior Leadership Team to ensure it reflects the latest statutory guidance and best practice in online safety.

Date agreed	11th September 2024
Review Date	10th September 2025
Approved by	Moinul Islam MBE (Head of Centre)
	Alaur Rahman (Head of Operations)

Path 4 AP is dedicated to fostering a safe, supportive, and respectful digital environment for all members of our community.