St Joseph's Catholic Primary School

Our Mission Statement

We grow together in God's Love as we Pray, Learn and Play

"Dyn ni'n tyfu gyda'n gilydd mewn cariad Duw wrth i ni weddïo, dysgu a chwarae"

INTERNET SECURITY POLICY

Article 32:

You have the right to be protected

This Policy was approved by the Governing Body on	September 2024	The first policy was drawn up and ratified by the Governing Body	Signed:
This policy is due to be reviewed by the Governing Body	February 2025	This Policy was reviewed by the Governing Body and ratified	Signed:
This policy is due to be reviewed by the Governing Body	November 2026	This Policy was reviewed by the Governing Body and ratified	Signed:
This policy is due to be reviewed by the Governing Body		This Policy was reviewed by the Governing Body and ratified	Signed:

1. Purpose

St. Joseph's RC Primary School is committed to providing a secure, supportive, and positive online environment for our students, staff, and the wider school community. This Internet Safety and Acceptable Use Policy aims to educate, protect, and empower everyone within our school to safely and responsibly use digital technology in all forms. The policy is grounded in UK best practices and complies with guidance from the UK Safer Internet Centre.

2. Scope

This policy applies to all students, staff, volunteers, and visitors using the school's network, devices, and internet services, whether on or off school premises. The policy also covers the appropriate use of personal devices when accessing school resources.

3. Objectives

1. To educate students and staff on safe and responsible internet use.
2. To protect all users from inappropriate content, cyberbullying, online grooming, and other internet-related risks.
3. To empower students with digital literacy and encourage responsible online behaviour.
4. To establish robust reporting mechanisms for internet-related issues.

4. Roles and Responsibilities

- **Headteacher and Governing Body**: Ensure the policy is implemented and adhered to, and resources are available for internet safety education.
- **Designated Safeguarding Lead (DSL)**: Monitor online safety, handle any concerns, and work with external agencies as needed.
- **Cardiff Council** monitor usage, and manage technical aspects of online safety.
- **Teachers and Staff**: Educate and model safe internet behaviour, report incidents, and integrate digital literacy into the curriculum.
- **Students**: Follow internet safety rules, report any concerns, and take responsibility for their online actions.
- **Parents/Guardians**: Support the school's policy by reinforcing internet safety practices at home.

5. Digital Safety Education

1. **Curriculum Integration**: Online safety education will be embedded across the curriculum.
2. **Workshops and Assemblies**: Regular internet safety workshops and assemblies will cover topics such as cyberbullying, privacy, online reputation, and the risks of sharing personal information.
3. **Staff Training**: All staff members will receive annual training on current internet safety risks, policies, and procedures, ensuring they can support students effectively.

6. Acceptable Use of Digital Technology

For Pupils

1. **Purpose**: This Acceptable Use Policy (AUP) outlines the rules and responsibilities for pupils when using the school's technology, internet, and online resources to ensure a safe and respectful digital environment.
2. **Guidelines for Responsible Use**:
    - **School Devices and Networks**: Pupils should only use the school's devices and networks for educational purposes. Unauthorised access to restricted sites or inappropriate content is not permitted.
    - **Personal Devices**: Personal devices may only be used with staff permission and must follow school rules regarding internet use and online safety.

- **Online Behaviour**: Pupils should treat others with respect in all digital interactions. Cyberbullying, harassment, or unkind messages, whether within school networks or on personal devices, is strictly prohibited.
- **Privacy and Security**: Pupils must not share personal information (e.g., full name, address, phone number) online, especially with unknown individuals. Sharing personal login credentials is not allowed.
- **Content and Copyright**: Pupils should seek permission before copying or sharing any used with permission, and sources must be credited.

3. **Agreement**: All pupils are required to sign an Acceptable Use Agreement before being granted access to the school's network and digital resources. Violation of this policy may result in restricted access to school technology and additional disciplinary action as outlined in the school's behaviour policy.

For Staff and Volunteers

1. **Purpose**: This Acceptable Use Policy (AUP) provides clear guidance for staff on safe, responsible, and professional use of the school's digital resources to protect data, privacy, and the online wellbeing of all students and staff.
2. **Guidelines for Responsible Use**:
   - **School Devices and Networks**: Staff should use school devices and internet access primarily for educational and professional purposes. Personal use should be limited and not interfere with work responsibilities.
   - **Professional Conduct Online**: Staff are expected to model responsible online behaviour. Inappropriate, unprofessional, or unethical digital conduct, including language or images, is not acceptable.
   - **Data Protection**: All staff are responsible for maintaining data security in line with GDPR. Personal data related to students, staff, or school operations must only be shared through secure, approved methods.
   - **Personal Devices**: When using personal devices to access school resources, staff should follow the same privacy and security protocols as with school devices, including secure passwords and network encryption.
   - **Social Media**: Staff should maintain professionalism on social media, ensuring their posts reflect the standards expected by [School Name]. Posting images of students or disclosing sensitive school information is not permitted unless expressly approved.
3. **Monitoring and Compliance**: Staff use of the school's network may be monitored to ensure adherence to this policy. Any violations will be handled in accordance with the school's disciplinary procedures, and serious breaches may lead to legal action.
4. **Acknowledgement**: All staff members and volunteers must read and agree to the Acceptable Use Policy annually to maintain access to the school's technology and digital resources.

7. Zero Tolerance for Cyberbullying: Cyberbullying, including harassment, intimidation, or online abuse, is not tolerated and will be addressed promptly with appropriate consequences.

- **Encouraging Responsible Online Behaviour**: Students are encouraged to think critically, respect others, and consider the impact of their online actions. Digital citizenship and responsible conduct will be promoted across the curriculum.

8. Privacy and Personal Data Protection

- **Data Security**: Personal data must be protected in line with the Data Protection Act 2018 and GDPR regulations. Access to sensitive information will be restricted to authorised individuals only.
- **Digital Footprint Awareness**: Students will be educated on the importance of managing their digital footprint, privacy settings, and the potential long-term consequences of sharing personal information online.

9. Reporting and Responding to Incidents

- **Reporting Mechanism**: Students, staff, and parents are encouraged to report internet safety concerns to the DSL. Anonymous reporting channels are also available for students.
- **Incident Response**: The school will promptly investigate all reports, providing support as needed and involving external agencies when appropriate (e.g., Child Exploitation and Online Protection Centre, Local Safeguarding Children Board).
- **Record-Keeping**: Detailed records of internet safety incidents will be maintained and reviewed to identify trends and improve policies.

10. Parental Engagement and Support

The school will provide parents with regular updates and resources to help reinforce internet safety practices at home. This includes workshops, newsletters, and links to reliable internet safety resources.

11. Policy Review

This policy will be reviewed annually by the Governing Body in collaboration with the DSP, IT staff, and student representatives to ensure it remains current with new risks, technologies, and best practices.