Cybersecurity Policy
(Whole School including EYFS)

Independent Day School

Our Lady of Sion School

Last Reviewed:	August 2025
Frequency of Review:	Annually
Next Review Due:	August 2026

1. Policy Statement

This policy sets out the school's approach to protecting its digital systems, safeguarding sensitive data, and ensuring the safety and wellbeing of pupils, staff, and the wider school community.

It is written in accordance with:

- **Keeping Children Safe in Education (KCSIE) 2025**
- **Working Together to Safeguard Children (2025)**
- **DfE Digital and Technology Standards for Schools and Colleges**
- **UK GDPR & Data Protection Act 2018**
- **ISI Inspection Framework**

2. Scope

This policy applies to:

- All staff, governors, contractors, visitors, and volunteers using school IT resources.
- All pupils using school devices, networks, and online platforms.
- Third-party providers handling school data or systems.

3. Roles and Responsibilities

Governing Body

- Maintain oversight of cybersecurity risk management.
- Ensure compliance with statutory guidance and ISI requirements.
- Review policy annually.

Headteacher / Senior Leadership Team (SLT)

- Ensure resources are allocated for cybersecurity.
- Oversee implementation of this policy.

Designated Safeguarding Lead (DSL)

- Integrate cybersecurity within safeguarding policies.
- Monitor filtering/monitoring systems to protect children from harmful content (including misinformation, disinformation, conspiracy theories, and misuse of AI).

Bursar as Data Protection Officer (DPO) / IT Lead (Serval/Entrust)

- Conduct regular risk assessments.
- Ensure compliance with data protection law.
- Manage backups, updates, and technical safeguards.

All Staff

- Follow safe digital practices.
- Report suspicious emails, breaches, or IT concerns immediately.

Pupils

- Follow the school's acceptable use policy (AUP).
- Report concerns about online safety or suspicious activity.

4. Cyber Risk Assessment & Planning

- Risk assessments carried out **termly**, with a full annual review.
- Use **DfE's "Plan Technology for Your School"** self-assessment tool.
- Findings reported to the Governing Body.

5. Technical Controls

- **Firewalls & Network Security**
  - Firewalls installed, configured, and maintained.
- **Updates & Licensing**
  - All software licensed and regularly patched. Unsupported software prohibited.
- **Anti-Malware**
  - Approved antivirus/anti-malware installed on all devices.
- **Access Controls**
  - Role-based access with the principle of least privilege.
  - Multi-Factor Authentication (MFA) used for sensitive systems.
- **Backups & Recovery**
  - At least three copies of essential data, across two devices, with one off-site.
  - Backups tested regularly.
- **Business Continuity**
  - Cybersecurity incorporated into the school's disaster recovery plan.
  - Plans tested annually.

6. Filtering, Monitoring & Artificial Intelligence

- Filtering systems block harmful or inappropriate content.
- Monitoring systems reviewed annually for effectiveness.
- Systems explicitly address **misinformation, disinformation, and conspiracy theories** as safeguarding risks.
- Use of **Generative AI** in teaching or administration is subject to staff oversight and must not be used to make automated safeguarding decisions.

7. Training & Awareness

- **Staff & Governors**
  - Annual training on cyber risks, phishing, online safety, AI, and safeguarding integration.

- **Pupils**
    - Age-appropriate education on online safety, information credibility, and responsible technology use.
- **Culture of Awareness**
    - Promote vigilance, responsibility, and reporting across the school community.

8. Incident Response & Reporting

- **Internal Reporting**
    - All staff must report suspected cyber incidents immediately to the IT Lead or DSL.
- **Response Plan**
    - School maintains a Cyber Response Plan detailing escalation, communication, and recovery actions.
- **External Reporting**
    - Serious incidents reported to:
        - **Action Fraud** (for cybercrime)
        - **DfE** (if data or service continuity affected)
        - **ICO** (where personal data breaches occur)

9. Integration with Safeguarding

- Cybersecurity is a safeguarding issue under **KCSIE 2025**.
- Online harms (content, contact, conduct, commerce) are addressed.
- Safeguarding responsibilities apply when pupils use school technology in **alternative provision settings**.
- AI safeguarding measures include **human oversight at all times**.

10. Policy Review

- Reviewed **annually** by the SLT and Governing Body.
- Interim updates may be made to reflect changes in statutory guidance.
- Next review due: **July 2026**.

Approved by Board of Governors August 2025