Islamic School of Canberra

Cyber Security Policy

Applies to: Staff, Students, Parents/Carers, Volunteers, and Contractors

1. Purpose

The purpose of this Cyber Security Policy is to ensure that all members of our school community use digital technologies safely, responsibly, and in accordance with Islamic values, Australian law, and the school's duty of care.
This policy aims to:

- Protect students, staff, and families from cyber risks
- Safeguard school data, systems, and digital resources
- Promote responsible online behaviour grounded in amanah (trust) and akhlaq (good character)
- Establish clear expectations, procedures, and consequences

2. Islamic Values Guiding This Policy

Our approach to cyber safety is rooted in Islamic principles, including:

- **Amanah** – protecting information and using technology responsibly
- **Taqwa** – being mindful of Allah in all online actions
- **Respect and kindness** – avoiding harm, bullying, or misuse of digital platforms
- **Honesty** – avoiding plagiarism, cheating, or deception online

3. Scope

This policy applies to:

- All staff, students, parents/carers, volunteers, and contractors
- All school-owned devices, networks, platforms, and accounts
- Personal devices used on school grounds or for school-related activities
- All online interactions involving school community members

4. Definitions

- **Cyber Security:** Protection of digital systems, data, and users from harm or unauthorised access.
- **Cyberbullying:** Using digital platforms to harass, threaten, or harm others.
- **Personal Information:** Any information that identifies an individual (e.g., name, address, photos).
- **School Digital Services:** Email, portals, apps, cloud platforms, and school devices.

5. Roles and Responsibilities

5.1 School Leadership

- Maintain secure digital systems and ensure compliance with relevant legislation
- Provide training for staff and age-appropriate education for students
- Respond promptly to cyber incidents

5.2 Staff

- Model responsible digital behaviour
- Protect student data and follow privacy requirements
- Report cyber incidents immediately
- Use school systems for professional purposes only

5.3 Students

- Use technology respectfully and responsibly
- Protect their passwords and personal information
- Report unsafe or inappropriate online behaviour
- Follow teacher instructions regarding device use

5.4 Parents/Carers

- Support safe technology use at home
- Monitor children's online activity
- Report concerns to the school
- Avoid sharing school-related photos or information without permission

6. Acceptable Use Expectations

6.1 General Expectations

All community members must:

- Use digital tools for educational or authorised purposes
- Keep passwords private and secure
- Access only appropriate and approved websites
- Respect intellectual property and copyright

- Avoid downloading unauthorised software or apps

6.2 Prohibited Behaviours

The following are strictly prohibited:

- Cyberbullying, harassment, or spreading harmful content
- Accessing inappropriate, violent, or extremist material
- Sharing private information without consent
- Hacking, bypassing filters, or attempting to access restricted systems
- Using school devices for illegal or unethical activities
- Recording or photographing others without permission
- Creating or using social media accounts where the user is under the minimum age of 16 years old

7. Data Protection and Privacy

The school will:

- Store data securely and limit access to authorised staff
- Comply with the **Australian Privacy Principles (APPs)**
- Ensure third-party digital platforms meet privacy standards
- Require staff to use school-approved communication channels

Parents and students must not:

- Share login details
- Post identifiable school information publicly
- Upload student images without school approval

8. Cyberbullying and Online Misconduct

8.1 Definition

Cyberbullying includes:

- Hurtful messages, comments, or posts
- Sharing embarrassing images or videos
- Impersonation or fake accounts
- Excluding others online
- Threats or intimidation

8.2 Reporting

Students, staff, or parents must report incidents to:

- Homeroom teacher
- Behaviour Coordinator

- Wellbeing Coordinator
- Principal

Reports may be made in person, via email, or through the school's reporting form.

8.3 School Response

The school will:

- Investigate promptly and confidentially
- Support affected students
- Apply consequences as per the **Education Act**, school behaviour policy, cyber security policy and duty of care
- Notify parents and external authorities when required

9. Consequences for Breaches

Consequences depend on severity and may include:

- Verbal or written warnings
- Loss of device or network privileges
- Parent meetings
- Behaviour contracts
- Suspension (internal or external)
- Referral to external agencies (e.g., eSafety Commissioner, Police) for serious breaches

All consequences will be applied fairly, consistently, and in line with Islamic values of justice and accountability.

10. Cyber Safety Education

The school will provide:

- Age-appropriate digital citizenship lessons
- Workshops for parents
- Staff professional learning
- Awareness campaigns promoting safe online behaviour

11. Use of Personal Devices (BYOD)

Where permitted, students may use personal devices under the following conditions:

- Devices must be used only for learning
- Mobile phones are not permitted while on school premises. They need to be handed to office until end of the day
- Personal hotspots are prohibited
- Devices must connect only to the school's filtered network

12. Social Media Guidelines

Students and parents must not:

- Create unofficial school pages or groups
- Post images of students without consent
- Engage in negative or defamatory comments about school, staff or students
- Contact staff through personal social media accounts
- Allow children under 16 to create or use social media accounts including but not limited to INSTAGRAM, SNAPCHAT, TIKTOK, FACEBOOK, X, AND YOUTUBE.
- Use social media to communicate about school matters in a way that breaches privacy, safety or school values.

Staff must follow professional boundaries and use only school-approved communication channels.

13. Incident Response and Recovery

In the event of a cyber incident (e.g., data breach, hacking attempt), the school will:

- Secure affected systems
- Notify leadership and relevant authorities
- Communicate with affected individuals
- Restore systems safely
- Review and strengthen security measures

14. Review of Policy

This policy will be reviewed every **three years** or earlier if required due to legislative changes, emerging risks, or technological developments.

Version: 26	
Approved by Board member/director	Ahmadullah Sadi
Signature	
Approval Date	02 June 2026