A simple checklist for your school

Security posture: how strong are your current defences?

- [ ] Devices and systems are patched and up to date
- [ ] MFA is used for all privileged (admin user) access and for all users accessing sensitive data where possible
- [ ] Staff receive regular online security training
- [ ] Strong password and access policies are in place
- [ ] Risks are reviewed regularly
- [ ] Compliance requirements are understood and met
- [ ] Leadership responsibility: set expectations, approve policies, provide staff training
- [ ] Technical responsibility: set up security controls correctly, apply updates, patches regularly, monitor systems for alerts, vulnerabilities, and unusual activity.

Security resilience: can you recover quickly when needed?

- [ ] Incident response plan is documented and tested
- [ ] Roles and responsibilities during a cybersecurity incident are clear
- [ ] Backups are frequent, secure, and regularly tested
- [ ] A business continuity plan supports teaching and administration
- [ ] Recovery processes are practised, not just documented
- [ ] Leadership responsibility: ensure plans exist, lead communication, support recovery efforts
- [ ] Technical responsibility: manage backups, test recovery, coordinate incident response.