OXFORDAQA
INTERNATIONAL QUALIFICATIONS

Cyber Security for OxfordAQA Schools

Protecting exams, students and data

Use Strong Passwords

- Create a strong, unique password for **every** account you use.
- Use **three random words** or another creative method to make passwords long and hard to guess (e.g., *OrangeTrainWindow*).
- Never use easy-to-guess passwords like birthdays, names, school names, or simple patterns.
- Do **not** reuse the same password on different systems.
- Turn on **two-step verification / two-factor authentication (2FA)** or **multi-factor authentication (MFA)** wherever possible.

Never Share Your Passwords

- Keep all passwords and authentication codes **private**—never share them with colleagues or students.
- Do not write passwords in places others can see (e.g., sticky notes, notebooks, shared folders).
- Always log out of accounts when using shared or public devices.

Be Alert to Phishing Emails

- Do not click on links or open attachments in emails that look unusual or unexpected.
- If an email seems suspicious, even if it appears to come from someone you know, **verify** it before taking action.
- Watch for spelling errors, urgent requests, or emails asking for login details.

Secure Your Devices

- Always lock your device (laptop, tablet, phone) when stepping away.
- Ensure your devices are encrypted and protected with a password or PIN.
- Install all software updates promptly.
- Keep antivirus and security tools up to date.

Use Secure Networks

- Avoid using public Wi-Fi for anything involving exam materials, student data, or confidential information.
- If you must use public Wi-Fi, always connect through a VPN.

Protect Data

- Back up important data regularly and store it securely.
- Only give access to sensitive data to members of staff who need it for their role.
- Ensure exam-related information is shared on secure systems - not through personal emails or messaging apps.

Stay Informed and Prepared

- Report suspicious activity or incidents to your IT team immediately.
- Ensure all staff receive regular cyber security training to stay updated on the latest threats and best practices.
- Check your country’s national cyber security guidance as well as OxfordAQA security procedures to ensure full compliance.
- Train staff and students on how to recognise and report phishing attempts.
- Develop and maintain a **contingency plan** so staff know what to do if a breach occurs.

OxfordAQA Reminder

- Protect all exam materials and student information at all times.
- Follow your school’s data protection, safeguarding, and IT policies.
- For any suspected breach affecting exam security, contact **OxfordAQA immediately:**

  Telephone: +44 (0)161 696 5995

  Email: info@oxfordaqa.com