

CYBER SECURITY

Staying safe when using email

Cyber security awareness for phishing, impersonation, malicious links, attachments and QR codes.

THE QUICK TEST

An email can look polished and still be malicious. Stop, verify the request using a trusted contact route and report concerns early.

Warning signs

- Urgency, secrecy, pressure or a threat of consequences.
- A payment, payroll or bank-detail change.
- A request for a password, MFA code or unexpected sign-in.
- An unusual link, attachment, shared file or QR code.
- A familiar display name but a different address or domain.
- A message that is plausible but unexpected for your role.

Stop and check

- Do not click, reply, scan the QR code or enable content.
- Check the full sender address and where a link really leads.
- Contact the person using a known number or directory entry - not the details in the message.
- Use the school's Report Phishing button or approved reporting route.
- For payment changes, use the finance team's independent verification process.

If you clicked or responded

- Contact IT immediately and say exactly what happened.
- If you entered a password, use the genuine service to change it and tell IT.
- If money or bank details are involved, alert Finance and the bank immediately.
- Do not wait for symptoms and do not hide an honest mistake.
- Keep the message unless IT asks you to remove it.

Safer everyday habits

- Use MFA and never approve a prompt you did not initiate.
- Open important services from a saved bookmark or trusted portal.
- Be cautious with unexpected document-sharing and voicemail notices.
- Keep work information off personal accounts unless school policy permits it.
- Report near misses - they help protect colleagues and pupils.

REMEMBER

Remember: genuine colleagues and suppliers will understand a security check. If the message reached a work device or account, your IT team should be told even when you did not click.

AUTHORITATIVE GUIDANCE

NCSC: [How to spot and report phishing scams](#)

NCSC: [If you have shared sensitive information](#)

NCSC: [Report a suspicious email](#)

Guidance checked 22 August 2026. Follow your school's incident and phishing-reporting procedures. This guide does not replace instructions from your IT or safeguarding team.