

Online Safety and Social Networking Policy

1. Introduction

The Procurement Academy is committed to safeguarding all learners, staff, and stakeholders when using online technologies. This policy provides guidance on safe and responsible use of the internet, social media, and electronic communication and takes into account the DfE statutory guidance “keeping children safe in Education” which is updated annually. While information and communication technology (ICT) is essential for employment, education, and lifelong learning, it can also present risks, particularly for vulnerable individuals. These risks can be categorised into three main areas:

- **Content** – exposure to illegal, inappropriate, or harmful material.
- **Contact** – harmful online interaction with other users.
- **Conduct** – personal online behaviour that causes or increases the likelihood of harm.

2. Policy Aims

- 2.1 Ensure all staff, learners and apprentices can work and study safely in an environment free from discrimination.
- 2.2 Balance individual rights to education with safeguarding responsibilities.
- 2.3 Prepare students for modern workplace demands, including safe online research and communication.
- 2.4 Provide clear guidance on acceptable and safe use of online technologies and social media.

3. Scope

- 3.1 This policy applies to all staff, learners, apprentices, and visitors to The Procurement Academy.
- 3.2 It covers all forms of online communication, including social media platforms, websites, messaging apps, mobile devices, and email.

4. General Online Safety Principles

- Be respectful, professional, and lawful in all online activity.
- Do not share personal information (yours or others’) without consent.

- Avoid explicit, extremist, or abusive content.
- Use privacy settings and only connect with people you know.
- Protect your passwords and devices; report security concerns immediately.
- Follow The Procurement Academy's safeguarding policies at all times.

5. Social Media Guidelines

- Avoid posting anything you wouldn't want a tutor, employer, or recruiter to see.
- Never post sexually explicit, abusive, or discriminatory material.
- Do not engage in radicalisation or extremist activity online or anywhere else.
- Check privacy settings and set personal profiles to "private."
- Do not accept friend/follow requests from unknown individuals.
- Avoid accessing personal social media in public learning spaces.
- Protect against identity theft — do not share security-question details (e.g., date of birth, place of birth, favourite team).
- Change passwords regularly and never share them.
- Do not post your current location; wait until you return home before sharing travel photos.

6. Security & Safe Technology Use

6.1 Cookies

- Understand cookies store browsing data; some track behaviour.
- See [Get Safe Online – Cookies](#) for more.

6.2 Security on the Move

- Treat mobile devices like wallets; do not leave unattended.
- Use PIN/password, encryption, and remote wipe.
- Keep software updated.
- Wipe data securely before disposing of old devices.
- See [Get Safe Online – Mobile Devices](#).

6.3 Passwords

- At least 8 characters, with upper/lowercase, number, and special symbol.
- Use different passwords for each account.
- Never share passwords.
- Change immediately if compromised.

6.4 Phishing & Fraud

- Watch for urgent requests, unknown senders, suspicious links, or unexpected attachments.
- Hover over links to check authenticity.
- Phishing can happen by email, text, call, or social media.
- See [Get Safe Online – Phishing](#).

6.5 Banking & Online Shopping

- Only use trusted websites (look for HTTPS and padlock icon).

- Avoid public Wi-Fi for payments.
- Check bank statements regularly.
- Never send money to unknown individuals online.
- See [Get Safe Online – Shopping & Banking](#).

6.6 Device & Computer Safety

- Keep antivirus software up to date.
- Log off or lock devices when not in use.
- Do not leave personal devices unattended.

7. Reporting Concerns

If you see or experience unsafe, abusive, or illegal online behaviour:

- Report immediately to your employer, tutor or designated safeguarding officer.
- If applicable, use helplines such as the Revenge Porn Helpline.

8. Useful Resources

- [Get Safe Online](#) – online safety tips.
- [Money Advice Service](#) – safe shopping guidance.
- UK Safer Internet Centre – education resources.

Appendix A: Enabling Google Safe Search

1. Go to browser settings (gear icon).
2. Select Search Settings.
3. Tick Turn on Safe Search.
4. Click Save.

DOCUMENT CONTROL

VERSION	DATE OF ISSUE	DATE OF REVIEW	DATE OF NEXT REVIEW	SIGNATURE
4	June 2021	August 2025	August 2026	<i>Philip Chippindale</i>