IT, Data Protection & Social Media Policy

1. Policy Statement

Hughes Driver Training is committed to ensuring the responsible, secure, and lawful use of its IT systems, safeguarding personal data, and protecting the company's reputation both online and offline.

All employees, contractors, and learners are expected to use IT resources and social media responsibly and in line with this policy.

---

2. Scope

This policy applies to:

- All employees, contractors, learners, and visitors using company IT systems.
- All use of company email, networks, devices, software, and internet access.
- All social media activity that references or could impact Hughes Driver Training.

---

3. IT & Systems Use

- Company IT resources are provided for legitimate business purposes.
- Keep passwords secure, do not share them, and change them regularly.
- Do not install unauthorised software or access offensive, illegal, or inappropriate material.
- Company IT systems may be monitored for security and compliance.
- Use only approved communication platforms when dealing with company business.

---

4. Data Protection (GDPR Compliance)

We comply with the **UK General Data Protection Regulation (GDPR)** and the **Data Protection Act 2018**.

- Personal data must be collected and used only when necessary and for a lawful purpose.
- Store data securely — lock screens, use password protection, and avoid leaving documents unattended.
- Do not share personal data outside the company unless authorised and legally compliant.
- Report any actual or suspected data breach to the Data Protection Officer (DPO) immediately.
- Dispose of confidential data securely, using shredding or secure deletion methods.

---

5. Social Media Use

Professional Use:

- Only authorised staff may post on official company social media accounts.
- All content must be accurate, respectful, and in line with company branding and values.
- Do not post confidential, sensitive, or commercially sensitive information.

Personal Use:

- Personal social media activity must not bring the company into disrepute or damage its reputation.
- Do not disclose confidential information or use the company logo without permission.
- Avoid engaging in online disputes or making comments that could be perceived as discriminatory, offensive, or harassing.

- At no point must you use candidates photos without their permission

---

6. Security Measures

- Use multi-factor authentication where possible.
- Keep software and security patches up to date.
- Do not connect unauthorised devices to company networks.
- Report phishing attempts, suspicious emails, or unusual system activity immediately.

---

7. Breaches of Policy

- Employees: breaches may result in disciplinary action up to and including dismissal.
- Learners: breaches may result in removal from the training programme.

- Serious breaches involving data protection or cybercrime may result in legal action.

---

8. Monitoring & Review

This policy will be reviewed annually or sooner if there are changes in legislation, technology, or operational needs.

V1 - Document Owner: Rosie Richardson
Effective Date: Sept 2025
Next Review Date: Sept 2026