

E-Safety and Digital Safeguarding Policy

Organisation: GLAS Business Solutions

Policy Owner: Designated Safeguarding Lead (DSL)

Applies to: All staff, associates, contractors and learners

Version: 1.1

1. Policy Statement

GLAS Business Solutions recognises the benefits that digital technology brings to teaching, learning, communication and business operations. The organisation is committed to ensuring that digital technologies are used **safely, responsibly and respectfully**, and that risks associated with online activity are managed proportionately.

This policy supports the organisation's wider **Safeguarding and Prevent responsibilities** and applies to all learning and professional activity involving digital technologies.

2. Scope and Context

GLAS Business Solutions delivers training and assessment primarily to **adult learners aged 19+**, through:

- Workplace-based delivery
- Remote and online platforms
- Digital communication and systems

E-safety risks within this context relate primarily to:

- Online behaviour and conduct
- Exposure to harmful or illegal online content
- Cyber-bullying or harassment
- Data security and misuse of digital systems
- Online radicalisation risks

This policy applies to:

- Organisation-owned digital systems and platforms
- Personal devices when used to access GLAS systems or provision

3. Definition of an E-Safety Incident

An e-safety incident is any activity using digital technology that:

- Places an individual's **personal safety, wellbeing or financial security** at risk
- Involves harassment, bullying or threatening behaviour
- Involves access to illegal, extremist or inappropriate content
- Breaches data protection, confidentiality or acceptable use standards

4. Responsibilities

All Staff, Associates and Contractors

- Use digital systems responsibly and professionally



- Maintain appropriate online boundaries with learners
- Report any actual or suspected e-safety concerns promptly

Learners

- Use digital platforms responsibly and respectfully
- Report any concerns relating to online safety or conduct
- Refrain from behaviour that could harm others or themselves

Designated Safeguarding Lead (DSL)

- Receives and records e-safety concerns
- Determines appropriate action and escalation
- Liaises with external agencies where required

5. Reporting and Managing Concerns

All e-safety concerns must be reported to the **Designated Safeguarding Lead** without delay.

The DSL will:

- Record the concern in line with safeguarding procedures
- Assess risk and decide proportionate action
- Escalate to external agencies where required (e.g. Prevent, police)
- Ensure appropriate support is provided

E-safety concerns are managed in line with the **Safeguarding Policy** and **Prevent Duty procedures**.

6. Online Conduct and Professional Boundaries

GLAS Business Solutions expects all staff and learners to:

- Communicate respectfully in online and digital environments
- Avoid inappropriate, offensive or discriminatory content
- Maintain professional boundaries in all digital communication

Cyber-bullying, harassment or misuse of digital platforms will not be tolerated and may result in disciplinary or contractual action.

7. Illegal or Harmful Online Content

Where concerns arise regarding:

- Illegal online material
- Extremist or radicalising content
- Threats of harm to self or others

These will be treated as **safeguarding matters** and managed in line with statutory guidance and organisational procedures. Staff must not download, copy or share illegal content under any circumstances.

8. Data Protection and Digital Security

Use of digital systems must comply with **UK GDPR and Data Protection legislation**.

Users must:

- Protect login credentials
- Avoid unauthorised sharing of information
- Use approved systems and platforms

Suspected data breaches must be reported immediately in line with the organisation's data protection procedures.

9. Training and Awareness

All staff receive:

- Safeguarding and Prevent training, including online safety awareness
- Updates where risks, technology or guidance changes

Learners receive appropriate guidance during induction on:

- Acceptable online behaviour
- Reporting concerns

10. Monitoring and Review

This policy is reviewed:

- **Annually**, or
- Earlier if technology, guidance or organisational activity changes

Formal approval, version control and review dates are managed through the organisation's policy register.