

2026

KMP 009 Data Protection Policy



Policies and Procedures

GHL DATA PROTECTION POLICY

1. Policy Statement

Group Horizon Ltd is committed to protecting the privacy, confidentiality, and integrity of personal data. The organisation processes personal data in accordance with the UK General Data Protection Regulation (UK GDPR) and the Data Protection Act 2018.

This policy sets out how Group Horizon Ltd ensures that personal data is handled lawfully, fairly and transparently while maintaining the highest standards of security and accountability.

Group Horizon Ltd recognises the importance of safeguarding the personal information of learners, employers, staff, and other stakeholders.

2. Scope of the Policy

This policy applies to all personal data processed by Group Horizon Ltd including information relating to:

- apprentices and learners
- prospective learners
- employers and employer representatives
- employees and job applicants
- subcontractors and delivery partners
- suppliers and contractors
- website users and prospective customers
- visitors to organisational premises where CCTV or doorbell camera systems operate
- audio, video and digital communications including recorded online teaching sessions, learner reviews and virtual meetings

The policy applies to all staff, contractors and associates who process personal data on behalf of the organisation.

3. Definitions

Personal Data

Information relating to an identified or identifiable individual.

Special Category Data

Sensitive personal data including:

- racial or ethnic origin
- health data
- disability information
- religious beliefs
- sexual orientation
- biometric data

Processing

Any operation performed on personal data including collection, storage, use, sharing or deletion.

4. Data Protection Principles

Group Horizon Ltd adheres to the seven principles of UK GDPR.

Personal data will be:

1. Processed lawfully, fairly and transparently
2. Collected for specified, explicit purposes
3. Limited to what is necessary
4. Accurate and kept up to date
5. Retained only as long as necessary
6. Processed securely
7. Processed in a way that demonstrates accountability

5. Lawful Basis for Processing

Group Horizon Ltd processes personal data under one or more lawful bases under Article 6 UK GDPR.

These include:

Contract

Processing necessary to deliver training services, apprenticeship programmes and contractual obligations with learners or employers.

Legal Obligation

Processing required to comply with legal or regulatory requirements including:

- Education and Skills Funding Agency (ESFA)
- HMRC
- safeguarding legislation
- health and safety requirements

Legitimate Interests

Processing necessary for organisational management and service delivery where this does not override individual rights.

Consent

Where individuals have provided clear permission for specific processing activities such as marketing communications.

Public Task

Processing related to publicly funded training programmes.

6. Special Category Data

Group Horizon Ltd may process special category data where necessary for:

- safeguarding learners
- supporting additional learning needs or reasonable adjustments
- equality monitoring and reporting requirements
- health and safety obligations

This processing is carried out in accordance with **Article 9 UK GDPR** and **Schedule 1 of the Data Protection Act 2018**.

Recording will normally cease at the end of the session. However, where participants remain within the session environment, any continued recording will be treated as part of the same session and managed in accordance with this policy.

Access to such data is restricted to authorised staff only.

7. Individual Rights

Individuals whose data is processed by Group Horizon Ltd have the following rights:

- The right to be informed
- The right of access (Subject Access Request)
- The right to rectification
- The right to erasure
- The right to restrict processing
- The right to data portability
- The right to object
- Rights relating to automated decision making

Requests relating to these rights should be submitted to the organisation's Data Protection Lead.

Group Horizon Ltd maintains a separate Subject Access Request Procedure which outlines how requests are received, verified, logged, processed, redacted and responded to in accordance with UK GDPR requirements.

Subject Access Requests will normally be responded to within one calendar month unless an extension is permitted under data protection legislation.

Where personal data is requested in connection with a complaint or appeal, this will be managed separately under the Subject Access Request procedure.

8. Data Sharing

Group Horizon Ltd may share personal data with relevant third parties where necessary for training delivery and regulatory compliance.

This may include:

- Department for Education
- Education and Skills Funding Agency (ESFA)
- awarding organisations
- end point assessment organisations
- employers of apprentices
- regulators including Ofsted
- subcontractors and delivery partners

All data sharing will comply with UK GDPR and appropriate data sharing agreements will be in place where required.

CCTV or doorbell camera footage will only be accessed where necessary for legitimate business purposes including security, safeguarding, health and safety, or incident investigation. Footage will only be shared with third parties, including law enforcement agencies, where there is a lawful basis to do so.

Online teaching platforms, virtual meeting systems and collaboration tools may process audio, video, chat and shared content as part of training delivery, learner reviews, quality assurance, safeguarding or operational activities. Access to recordings or communications will be restricted to authorised individuals and retained only where there is a legitimate organisational purpose.

9. Data Processors

Where external organisations process personal data on behalf of Group Horizon Ltd, they are considered **data processors**.

Examples may include:

- learning management systems
- e-portfolio platforms
- IT service providers
- cloud storage providers

Appropriate **Data Processing Agreements** will be established with all processors to ensure compliance with Article 28 UK GDPR.

10. Data Security

Group Horizon Ltd implements appropriate technical and organisational measures to protect personal data.

These include:

- secure IT systems and networks
- password and access controls
- encryption and secure storage
- restricted access to sensitive data
- secure document disposal procedures
- staff training on data protection
- secure management of CCTV and doorbell camera footage and access permissions
- secure management of online meeting platforms, recordings, transcripts and digital communications

All staff are responsible for protecting personal data they process.

11. Personal Data Breaches

A personal data breach is any incident that leads to accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data.

All suspected breaches must be reported immediately to the **Data Protection Lead**.

Where a breach is likely to result in risk to individuals' rights and freedoms, Group Horizon Ltd will notify the **Information Commissioner's Office (ICO)** within **72 hours** of becoming aware of the breach.

Affected individuals will also be informed where required.

12. Data Retention

Personal data will only be retained for as long as necessary to fulfil the purpose for which it was collected.

Retention periods are set out in the organisation's **Data Retention Schedule**.

Typical retention periods include:

- learner records 6 years after completion
- funding evidence 6 years
- staff records 6 years after employment ends

Data will be securely deleted or destroyed once retention periods expire.

CCTV and doorbell camera recordings will normally be retained only for a limited period in accordance with system settings unless required for investigation, safeguarding, legal or insurance purposes.

Recordings or transcripts of online teaching sessions, learner reviews, meetings or digital communications will only be retained for as long as necessary for training delivery, quality

assurance, safeguarding, compliance or operational purposes in accordance with the organisation's retention schedule.

Organisational records relating to learners and employers must be stored within approved organisational systems such as the learning management system or designated SharePoint locations. Personal storage locations such as individual devices or personal cloud storage must not be used for long-term storage of organisational data.

13. Artificial Intelligence and Automated Processing

Where technologies such as artificial intelligence or automated decision-making are used to process personal data, Group Horizon Ltd will ensure that such processing complies with UK GDPR and ICO guidance.

Appropriate safeguards will be implemented to protect individuals' rights.

Staff must not input confidential, safeguarding, special category or commercially sensitive personal data into unauthorised artificial intelligence systems or platforms.

14. Responsibilities

All staff must:

- comply with this policy
- handle personal data securely
- report suspected data breaches
- complete data protection training where required

Managers are responsible for ensuring that staff understand and follow data protection requirements.

15. Data Protection Lead

Group Horizon Ltd has appointed a **Data Protection Lead** responsible for overseeing compliance with data protection legislation.

The Data Protection Lead is responsible for:

- monitoring compliance
- advising on data protection obligations
- handling subject access requests
- managing data breach responses
- liaising with the ICO where necessary
- maintaining the SAR register
- overseeing redactions and exemptions
- ensuring lawful disclosure

- determining appropriate disclosure, redactions and application of exemptions under data protection legislation

Contact:

Karen Nichols

Data Protection Lead

Email: communications@grouphorizon.co.uk

16. Monitoring and Review

This policy will be reviewed **annually** or sooner if required due to:

- legislative changes
- regulatory updates
- organisational changes
- identified risks or incidents

17. Related Policies

This policy should be read alongside:

KMP 009A Privacy Policy

KMP 002 Safeguarding Policy

KMP 004 Data Retention and Disposal Schedule