Information Security Policy

Technical and organisational security requirements

Document owner	Rosie Aylward – Director and Data Protection Lead
Approved by	Director
Version	1.0
Approval / issue date	14 July 2026
Next review	14 July 2027
Status	Policy for approval and staff communication

Core standard
Personal information must be accessed only through approved accounts, systems and devices. Identifiable learner, safeguarding, health or staff information must not be stored in personal email, consumer messaging, personal cloud storage or public AI tools.

1. Purpose and scope

This policy sets minimum security requirements for staff, contractors and volunteers using Compass systems, devices, email, paper records and premises. It applies wherever work is undertaken, including the shared church-house site, home working, travel and educational visits.

2. Responsibilities

- The Director and Data Protection Lead approve systems, risk decisions and access.
- The DSL controls access to safeguarding records and considers welfare implications of incidents.
- All users protect credentials and devices, follow approved methods and report concerns immediately.
- Suppliers must meet contractual security standards and report incidents without undue delay.

3. Approved systems and accounts

- Only approved business systems may be used for personal information.
- Each user must have an individual account. Shared accounts are prohibited unless technically unavoidable, risk assessed and subject to compensating controls.
- Administrator rights must be limited to those who need them and reviewed regularly.
- New systems, integrations and apps require supplier due diligence and DPIA screening before use.

4. Passwords and multi-factor authentication

- Use a unique strong passphrase for each business account and store it only in an approved password manager where one is provided.
- MFA must be enabled wherever available, including Webador administrator and email-related accounts.
- Passwords, one-time codes and recovery details must never be shared or sent in the same message as protected information.
- Suspected compromise must be reported immediately and credentials changed from a trusted device.

5. Webador business email and Outlook

- The authorised mailbox is info@compass-learning.co.uk, hosted by Webador and accessed through approved Outlook configurations.
- Outlook may cache email and attachments locally. Only encrypted, password-protected authorised devices may be connected.
- Automatic forwarding to personal accounts is prohibited. Mail rules and connected devices must be reviewed periodically.
- Sensitive attachments should be replaced by secure links/portals where available. Where a protected file is necessary, send the password by a separate method.
- Avoid sensitive information in subject lines and verify every recipient, attachment and reply-all list before sending.
- Deleted Items, Junk, downloads and local archives must be managed in line with the retention schedule.

6. Devices and mobile working

- Business devices must use supported operating systems, automatic security updates, malware protection, encryption, strong passcodes and automatic locking.
- Devices must not be shared with unauthorised family members or other users.
- Lock screens and hide sensitive notification previews. Keep devices physically secure and never leave them visible in a vehicle.
- Personal devices may not process identifiable learner or safeguarding data unless expressly approved, risk assessed and configured to the same standard.
- Loss, theft or suspected access must be reported immediately so accounts can be disabled and remote action considered.

7. Access control

- Access is based on least privilege and need to know.
- Safeguarding, medical and HR records must be separately restricted.
- Access rights are reviewed at least termly and when a role changes.
- Leavers' access is removed promptly; devices, keys and records are recovered; forwarding and shared credentials are reviewed.

8. Secure sharing and communication

- Confirm identity, authority, purpose, lawful basis and minimum necessary information before sharing.
- Use approved secure portals, encrypted links or professional email accounts. Confirm receipt for safeguarding and formal record transfers.
- Do not use WhatsApp, SMS, social media direct messages or personal email for routine identifiable learner information.
- Safeguarding urgency must not be delayed by uncertainty: share necessary and proportionate information through the safest available route and record the decision.

9. Physical and paper security

- Minimise printing. Store paper in locked cabinets in secure areas and keep safeguarding records separately restricted.
- Apply a clear-desk approach and do not leave registers, reports or notes visible in teaching or communal areas.
- Use sealed folders when approved transport is unavoidable and maintain a transfer/sign-out record.
- Use cross-cut shredding or an approved confidential-waste provider for secure destruction.

10. Shared premises and visitors

- Learners and visitors must not have unsupervised access to areas containing confidential records or unlocked devices.
- Keys and access arrangements must be controlled and losses reported immediately.
- Confidential conversations must take place where they cannot reasonably be overheard.
- Visitor and contractor access to systems or records requires authorisation, supervision and confidentiality controls.

11. Backups, availability and business continuity

- Critical systems must have appropriate backup, resilience and recovery arrangements.
- Backups must be protected from unauthorised access and ransomware and restoration must be tested periodically.
- Essential emergency, safeguarding and contact information must remain available through proportionate continuity arrangements.
- System outages and data unavailability must be reported and recorded where they affect confidentiality, integrity or availability.

12. Removable media, downloads and printing

- Unencrypted USB drives are prohibited. Removable media may be used only where approved and encrypted.
- Download information only where necessary, store it in the approved location and remove temporary copies promptly.
- Collect printing immediately and use secure printing where available.

13. AI and emerging technology

- Do not enter identifiable or pseudonymised learner, safeguarding, health, workforce or commissioner information into public generative AI or unapproved transcription/automation tools.
- Any proposed AI use requires a documented purpose, supplier assessment, lawful-basis review, DPIA screening, transparency review and Director approval.
- AI output must not be treated as an authoritative record or used for significant decisions without appropriate human review.

14. Security monitoring, incidents and breaches

- Users must immediately report phishing, malware, misdirected email, lost records, suspicious login alerts, unauthorised access and availability incidents.
- The Personal Data Breach Procedure applies. Evidence must be preserved and staff must not conceal incidents or contact affected people without authorisation.
- Security logs may be reviewed for legitimate security, compliance and investigation purposes in accordance with privacy information.

Appendix A – Minimum technical standard

Area	Minimum requirement
Accounts	Individual accounts; least privilege; MFA wherever available; prompt leaver removal.
Devices	Encryption; strong passcode; supported OS; updates; auto-lock; malware protection.
Email	Approved mailbox/client; no personal forwarding; recipient check; secure attachments/links.

Area	Minimum requirement
Cloud systems	DPA; approved locations/transfer; access logs; backups; recovery; deletion terms.
Paper	Minimise; locked storage; clear desk; sealed transfer; confidential destruction.
Remote work	Private environment; secure connection; no shared access; screen and conversation privacy.
Incident response	Immediate reporting; containment; controller notification; breach log.

Signed by Director: R.Aylward **Date: 14.07.26**

References and linked guidance

- **ICO: A guide to data security:** https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/security/a-guide-to-data-security/
- **ICO: Personal data breaches:** https://ico.org.uk/for-organisations/report-a-breach/personal-data-breach/personal-data-breaches-a-guide/
- **DfE: Data protection in schools:** https://www.gov.uk/guidance/data-protection-in-schools