Information Security Policy

Technical and organisational security requirements

Document owner	Rosie Aylward – Director and Data Protection Lead
Approved by	Director
Version	2.1
Approval / issue date	08.10.26
Next review	08.10.27, or sooner if required
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

Compass protects the confidentiality, integrity and availability of personal information held about learners, families, Compass staff and partners. This policy applies to all Compass staff and anyone authorised to use Compass information, whether working at a centre, school, home, community venue or remotely. It covers electronic and paper records, devices, conversations and all approved systems. The controls are proportionate to the sensitivity and risk of the information, particularly safeguarding, health and education records.

2. Responsibilities and approved systems

The Director and Data Protection Lead approves systems, access, information sharing arrangements and security risks, and coordinates incidents. The Designated Safeguarding Lead (DSL) controls access to safeguarding information and considers any risk to a young person. All Compass staff must follow this policy, complete training, protect their credentials and report concerns immediately. System suppliers must be assessed and subject to appropriate data processing and security terms before personal information is uploaded.

The approved core systems are CPOMS for safeguarding records and Microsoft 365, including Outlook and SharePoint, for business communication and controlled document storage. Personal email, personal cloud storage, consumer messaging and unapproved apps must not hold learner information. New systems, integrations or AI tools require approval, supplier assessment and a data protection impact assessment

(DPIA) screening before use. Compass records its role as controller or processor for each commissioned service and follows the applicable contract and data sharing arrangements.

3. Risk assessment and evidence of implementation

The Core Provision Data Protection Impact Assessment is the principal assessment of privacy and security risks for the core service. It must reflect current systems, delivery locations and working arrangements, including BYOD, sensitive children's information and remote working. The Director records risk owners, required actions, deadlines and residual risk decisions. It is reviewed at least annually, after a significant incident and before a material change. A supplementary assessment is required where a new activity or technical risk is not adequately covered. Processing must not start where required safeguards are absent; any remaining high risk is escalated for specialist advice and ICO prior consultation where required.

The Data Protection Operational Logs workbook provides supporting records. The Training Register records induction, declarations and annual refreshers; Supplier Due Diligence records contracts, security checks and decisions; the Access Review Log records permissions and account changes; and the Breach Log records incidents, notification decisions and lessons. The Data Sharing Log, Secure Transfer Log and Destruction Log evidence relevant disclosures, transfers and disposal. The DPIA Register links assessments and approvals, the Data Quality Log records corrections, and Management Actions tracks remedial work with owners, dates and closure evidence.

The Director reviews open management actions weekly and reconciles dashboard statements with underlying evidence. A blank log is a recording tool, not evidence that a control has been implemented. Completion status must reflect actual activity and available evidence; inconsistencies and obsolete system or premises references must be corrected. Logs must be access restricted, minimise sensitive detail and link to supporting evidence rather than store passwords or duplicate safeguarding accounts.

4. Accounts, authentication and access

Every member of Compass staff has an individual Microsoft 365 account with multi-factor authentication (MFA) enabled. Individual CPOMS accounts must also be used; MFA must be enabled where the service supports it. Shared accounts are prohibited. Strong, unique passwords or passphrases must be used, stored only in an approved password manager where provided, and never disclosed to colleagues. Administrative rights are restricted to named people and used only when required.

Access is granted by role and need to know, with separate restrictions for each learner's records and for safeguarding, health and staff information. The Director or delegated administrator approves access before it is granted, records the decision and reviews permissions at least termly and whenever an assignment changes. Access is removed promptly when a person leaves or no longer works with a learner. The review includes CPOMS, SharePoint sites and folders, Microsoft groups, guest access, shared links, devices and recovery methods. Staff must not use another person's account or leave an unlocked session unattended.

5. Storage in SharePoint and CPOMS

Safeguarding concerns, actions and chronology are recorded in CPOMS according to the Safeguarding Policy. Learner plans and other necessary personal documents are stored in restricted SharePoint locations, with access granted to named users for the learners they support. The SharePoint site and each learner folder must be checked for inherited permissions before use. Links should normally be restricted to specified people who authenticate; anonymous "anyone with the link" sharing must not be used for learner

or staff records. Editing, downloading, synchronisation and onward sharing are limited to what the role requires. The Director reviews access and sharing links regularly.

Where a document needs additional protection for an authorised transfer, it may be encrypted or password protected. The password must be strong and supplied through a different channel, such as a verified telephone call or an approved text to a confirmed number, rather than in a second email to the same mailbox. SharePoint protection relies on authenticated access permissions and the service's encryption controls; a separate document password is an additional measure where justified by the transfer risk. Staff must avoid duplicate copies and remove temporary downloads promptly. CPOMS and Microsoft 365 availability, export and recovery arrangements are documented and tested at a proportionate interval.

6. Email and information sharing

Compass staff use their own Microsoft 365 accounts for work. The Acceptable Use Policy requires staff never to use a child's full name in an email chain; initials are used instead. Initials do not make an email anonymous, especially when combined with a school, date or circumstances. Staff must therefore keep subjects and bodies brief, verify recipients and reply-all lists, use the minimum necessary detail, and share sensitive plans through restricted SharePoint access or another approved secure method. Where an unambiguous full identity is essential to safe action, it must be conveyed within the approved secure record or through a verified direct channel, with the decision recorded where appropriate.

Before sharing, staff confirm the recipient's identity and authority, the purpose, the minimum information needed and the relevant commissioning or data sharing arrangement. External access should use named recipients, authenticated links and expiry dates where suitable. Staff confirm receipt when transferring safeguarding or other critical records. Automatic forwarding to personal accounts and routine use of WhatsApp, SMS or social media for identifiable learner information are prohibited. An urgent safeguarding disclosure must not be delayed by uncertainty about the usual channel: staff use the safest available route, involve the DSL and document what was shared and why.

7. Bring Your Own Device

Compass staff may use a personally owned laptop, tablet or phone for Compass work only with the Director's approval. Before access is granted, the device must have a supported operating system, automatic security updates, device encryption where available, malware protection where appropriate, a strong passcode or biometric lock, automatic screen locking and a separate user profile if shared with others. Compass accounts must use MFA. Staff must not allow family members or other users to access a signed-in Compass account or learner information.

Staff should access CPOMS and SharePoint through approved apps or a browser and keep learner records in those systems. They must not save, sync, photograph, print or back up learner information to a personal account, local drive, camera roll or consumer cloud service. Any necessary temporary download must be approved, protected and deleted promptly. Compass may require the staff member to show that the device meets these conditions, remove Compass access or work data when an assignment ends, and cooperate with incident containment. Staff must report a lost, stolen, shared or compromised device immediately. If these conditions cannot be met, the device must not be used for Compass personal information.

8. Device configuration, firewalls and removable media

Before a device is approved, its owner must confirm supported software, enabled security updates, active malware protection appropriate to the operating system, an enabled host firewall where supported, and suitable encryption. Devices that cannot provide suitable protection must not process Compass personal information. Default credentials are changed, unnecessary software and services are removed or disabled, and routine work uses a standard account rather than administrator privileges wherever practicable. Critical security updates are prioritised according to risk; unsupported devices or software must be withdrawn from Compass use.

Networks controlled by Compass must use appropriately configured and updated router or boundary firewall protection. Administrative interfaces must be protected and unnecessary external access disabled. Where staff use home or hired-premises networks, they must use a trusted secured connection, keep device protections enabled and avoid untrusted public Wi-Fi for sensitive records; an approved secure connection or mobile hotspot should be used instead. Security features must not be disabled to gain access.

Removable storage, including USB drives and external disks, must not be used for personal information without prior Director approval. Approved media must be encrypted, recorded, securely stored, malware checked and used only for the authorised purpose. Unencrypted removable storage is prohibited for personal information. Lost media must be reported immediately.

9. Devices, remote work and premises

Devices used to access Compass systems must run supported software with automatic updates, malware protection, full-device encryption where available, a strong screen lock and automatic locking. Compass staff must keep devices and notification previews private, avoid shared family access, and report loss, theft or suspicious activity immediately. Public or shared computers must not be used for safeguarding or learner records. Staff should use a trusted connection and protect screens and conversations when working away from Compass premises.

Printing is minimised. Paper records are kept in locked storage, transported only when necessary in a sealed folder, and not left in teaching or shared areas. Staff collect printouts immediately and dispose of confidential waste by cross-cut shredding or an approved service. Learners, visitors and venue staff must not have unsupervised access to records or unlocked devices. Confidential discussions take place where they cannot reasonably be overheard.

10. Asset ownership, retention and secure disposal

The Director maintains or cross-references an asset register identifying approved hardware, software and cloud services, their owner, purpose and protection responsibilities. Approved personal devices are identified through the BYOD approval record without collecting unnecessary personal information. Information is classified by sensitivity: public information, internal business information and restricted personal information. Learner, safeguarding, health and workforce records require restricted access proportionate to their content.

Records are retained and deleted in accordance with the Data Retention and Secure Disposal Policy, commissioning terms and any legal hold. The Destruction Log records significant disposal decisions and evidence. Before a device is sold, recycled, reassigned, returned or repaired, the Director must approve

how Compass information, cached emails, downloads, tokens and saved credentials will be protected or securely removed. Deleting a file or emptying a recycle bin alone is not a reliable device sanitisation method. Use an appropriate verified secure erase, cryptographic erase or approved destruction service; retain relevant confirmation. Any backup copies follow documented retention and recovery arrangements.

11. Resilience, suppliers and assurance

The Director maintains an inventory of systems and devices, records the security and data processing terms for CPOMS and Microsoft 365, and reviews access, security settings, logs and supplier changes at least annually and after a material change. Critical information must be recoverable after accidental deletion, outage or cyber attack. Recovery arrangements, including any separate backup or export needed beyond supplier retention features, are documented and tested. A proportionate continuity method must preserve access to essential safeguarding contacts and information during an outage without creating uncontrolled copies.

Security measures are tested and reviewed in light of risk, including staff training, phishing awareness, access checks, device updates, restoration tests and incident learning. Staff must not enter identifiable or pseudonymised learner, safeguarding, health or workforce information into public generative AI or unapproved transcription tools. Any approved use requires a documented purpose, supplier assessment, DPIA screening and human review.

12. Training and security monitoring

All Compass staff complete information security, acceptable use, BYOD where relevant, phishing and breach recognition training before access to live personal information during induction. They acknowledge the relevant policies and complete refresher training at least annually and when significant changes or incidents require it. Completion, declarations and the next due date are recorded in the Training Register.

The Director or a named delegate checks available Microsoft 365 and CPOMS security alerts each working day and promptly investigates credible signs of compromise. Available sign-in, sharing, access and administrator activity logs are reviewed at least monthly and after a suspected incident, using a risk-based scope. Relevant logging and alerting must be enabled where supported; retention and licensing limitations are documented, and alternative controls are agreed where necessary. Review dates, findings and corrective work are recorded in Management Actions or the Access Review Log. Monitoring is proportionate and explained to staff through privacy information.

An annual security review evaluates permissions, device and firewall settings, supplier arrangements, training and recovery controls. It includes a documented recovery test and proportionate exercises for secure record transfer, account closure and device loss. The Director records what was tested, the result, actions, owners and completion evidence. Backup frequency, retention and acceptable recovery time are set according to the risk and need for continuity; cloud synchronisation alone must not be assumed to provide adequate backup.

13. Incidents and personal data breaches

Compass staff must report a misdirected email, lost device or paper, phishing attempt, compromised account, unauthorised access, deletion, malware or system outage to the Director and Data Protection Lead immediately, and to the DSL where a learner's welfare may be affected. They must preserve relevant evidence and follow instructions to contain the incident. The Personal Data Breach Procedure governs

assessment, notification and communication. Compass records every personal data breach, including decisions not to report. Where the legal threshold is met, the responsible controller reports to the ICO without undue delay and, where feasible, within 72 hours of awareness; individuals are informed without undue delay if the breach is likely to result in a high risk to them. Where Compass acts as processor, it alerts the controller without undue delay under the contract so that the controller can meet its duties.

14. Investigation and corrective action

Every confirmed breach must be investigated proportionately to establish what happened, its causes, affected information and people, and whether controls failed. Compass records containment, risk assessment, notification decisions and reasons, root cause and corrective actions in the Breach Log and, where necessary, Management Actions. Actions have an owner and deadline. The Director checks that actions are completed and effective, shares relevant learning with staff and updates training, the DPIA or policies as needed. A decision not to notify the ICO must be justified; notification is required unless the breach is unlikely to result in a risk to individuals' rights and freedoms. Delayed notification must be explained.

15. Review and related documents

This policy is reviewed annually and sooner after a significant incident, material technology change or change in law or guidance. It is read alongside the Data Protection Policy, Privacy Notices, Acceptable Use Policy, Retention Schedule, Safeguarding Policy, Data Sharing arrangements and Personal Data Breach Procedure. This policy sets the required standard; the Director records implementation and any approved exceptions with their risk controls.

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.
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.

These requirements apply alongside the controls in this policy and the approved risk assessments.

Appendix B BYOD approval record

Complete one record for each personal device before Compass access is granted. Store securely with the device/access records. Do not record passwords, recovery keys, biometric data or personal file contents. Approval applies only to the scope recorded below.

Staff name and role: _____

Device make/model and asset reference: _____

Operating system and version: _____

Systems and permitted use (including any approved local storage): _____

_____

Security check	Result	Evidence/date or action
Supported operating system and security updates enabled	Yes / No / N/A	
Strong lock and automatic screen locking enabled	Yes / No / N/A	
Encryption enabled and suitable for intended use	Yes / No / N/A	
Malware protection and firewall enabled where supported	Yes / No / N/A	
Compass MFA and individual accounts confirmed	Yes / No / N/A	
Separate user profile; no other person can access Compass sessions	Yes / No / N/A	
No personal cloud backup or unauthorised sync/downloads	Yes / No / N/A	
Loss reporting, privacy and account removal understood	Yes / No / N/A	
Any exceptions assessed and approved before access	Yes / No / N/A	

Outstanding actions / exceptions and risk controls: _____

_____

Staff declaration: I confirm the information above is accurate. I will follow Compass's Information Security and Acceptable Use Policies, report changes or incidents immediately, and remove Compass accounts and authorised local work data when instructed. Any required inspection or technical management must be explained and limited to a legitimate work security purpose; this approval does not authorise unrestricted access to my personal information.

Staff signature: _____ Date: _____

Decision: Approved / Approved with recorded conditions / Not approved

Approver and signature: _____ Approval date: _____

Next review date: _____ Access granted by: _____

Review at least annually and when the device, role or security status changes. Unresolved essential security checks prevent approval. Any technical monitoring or selective removal of work data must be explained before deployment; whole-device wiping is not authorised by this form.

Closure: Access revoked/date: _____ Work data removed/date: _____

Closure confirmed by: _____ Evidence: _____