# Compass Learning & Education

## Data Protection and Confidentiality Policy

| | |
|---|---|
| **Policy owner** | Director and Head of Provision - Rosie Aylward |
| **Data Protection Lead** | Rosie Aylward |
| **Approved by** | Director - Rosie Aylward |
| **Version** | 3.0 |
| **Approval date** | 01.10.26 |
| **Review cycle** | Annual, or sooner following a material legal, contractual, technological or operational change |
| **Date of next review** | 01.10.27 |

## 1. Purpose and Policy Statement

Compass Learning & Education recognises that learners, parents and carers, staff, commissioners and partners entrust the organisation with personal information. As an alternative provision supporting children and young people who may have SEND, SEMH needs, health needs or safeguarding histories, Compass processes information that can be particularly sensitive and capable of causing significant harm if it is inaccurate, unavailable or disclosed inappropriately.

Compass is committed to processing personal information lawfully, fairly, transparently and securely in accordance with the UK General Data Protection Regulation (UK GDPR), the Data Protection Act 2018 and other applicable law. This policy establishes the organisation's approach, responsibilities and minimum standards. Compliance is mandatory for every person processing personal information for or on behalf of Compass.

## 2. Scope

This policy applies to all personal information processed by Compass, whether recorded electronically, on paper, in email, in photographs or recordings, on approved devices, in safeguarding or learner systems, or through third-party services. It applies to information about:

- prospective, current and former learners;
- parents, carers and emergency contacts;
- employees, applicants, volunteers, contractors and visitors;
- school, academy trust, local-authority and professional contacts;
- suppliers, business contacts and individuals making enquiries, complaints or information-rights requests.

References to Compass staff in this policy include all people authorised to work on Compass's behalf. Biometric identity verification for recruitment is subject to the requirements in section 6.3. CCTV and any other new monitoring arrangements require a separate necessity assessment, DPIA screening, approval and updated privacy information before use.

## 3. Data Protection Principles

Compass will ensure that personal information is:

| Principle | Compass commitment |
|---|---|
| Lawfulness, fairness and transparency | Used only where a valid lawful basis and any additional condition have been identified, and individuals are told how their information is used. |
| Purpose limitation | Collected for specified, explicit and legitimate purposes and not used incompatibly with those purposes. |
| Data minimisation | Adequate, relevant and limited to what is necessary. |
| Accuracy | Accurate, clearly recorded and kept up to date where necessary. |
| Storage limitation | Kept only for as long as there is a lawful and documented need. |
| Integrity and confidentiality | Protected by appropriate technical and organisational measures. |
| Accountability | Supported by policies, registers, contracts, risk assessments, training, audit and evidence of decisions. |

## 4. Governance, Roles and Responsibilities

### 4.1 Director and Head of Provision

- holds overall accountability for data protection and information governance;
- approves this policy and ensures that sufficient resources, systems and training are provided;
- promotes a positive culture in which privacy, confidentiality and secure record keeping are part of everyday practice;
- reviews significant risks, incidents, audit findings and improvement actions.

### 4.2 Data Protection Lead

- advises the organisation and staff on data protection requirements;
- maintains the information asset, controller, processor, supplier and transfer records;
- coordinates DPIAs, information-rights requests, breach assessment, training and compliance reviews;
- acts as the main contact for the ICO, commissioners and individuals on data protection matters;
- records significant risks, decisions and corrective actions for management review. Where the Director also acts as Data Protection Lead, these decisions are documented and independent specialist advice is obtained where needed, including where a conflict of interest could impair objective review.

Compass has appointed a Data Protection Lead. It has not designated a statutory Data Protection Officer unless and until a documented DPO assessment determines that the legal threshold is met. The decision will be reviewed if the scale, duration or nature of processing materially changes.

### 4.3 Designated Safeguarding Lead

- ensures safeguarding records are accurate, restricted and shared only where necessary;
- advises on the safeguarding consequences of information incidents and disclosures;
- approves the transfer and disposal of safeguarding records where required.

### 4.4 All Staff and Contractors

- access and use personal information only where necessary for their authorised role;
- follow this policy, security requirements and commissioner instructions;
- keep records accurate, factual, respectful and timely;
- report requests, errors, loss, unauthorised access and suspected breaches immediately;
- complete required training and seek advice whenever uncertain.

## 5. Controller and Processor Roles

Compass will determine and document its role for each processing activity before personal information is accepted or used. The role is determined by who decides the purposes and essential means of the processing, not simply by the wording used in a contract.

- Compass is normally an independent controller for its workforce, recruitment, website, finance, complaints, legal claims, business administration and decisions it makes to comply with its own safeguarding, health and safety or other legal responsibilities.
- Compass may act as a processor where a school, academy trust or local authority commissions a service and determines the purposes and essential instructions for the learner information processed.
- Compass may have separate controller responsibilities for safeguarding, emergency action, legal compliance or service-quality decisions even where other placement activity is undertaken as a processor.
- When acting as processor, Compass will process information only on documented instructions unless required by law to do otherwise, and will inform the controller where legally permitted.
- Controller and processor roles, contacts, instructions, categories of processing, retention and end-of-contract arrangements will be recorded in the Controller Register and relevant written agreement.

## 6. Lawful Bases and Sensitive Information

Before processing begins, Compass will identify and document the applicable Article 6 lawful basis. The basis must reflect the particular purpose and the capacity in which Compass is acting. Potential bases include contract, legal obligation, vital interests and legitimate interests. Public task will only be used where the specific task or official authority is laid down by law and Compass can demonstrate that the processing is necessary and proportionate.

Consent will not be used where an individual does not have a genuine choice, or where Compass needs to continue the processing despite withdrawal. Consent may be appropriate for optional uses such as particular marketing photographs or communications, subject to separate assessment.

Where ordinary legitimate interests is relied upon, Compass will record the purpose, necessity and balancing assessment, giving particular weight to children's rights and expectations. Recognised legitimate interests may be used only where the precise statutory conditions apply; this does not remove the need for an Article 9 condition where special category information is involved. The processing register records the selected basis and supporting reasoning.

Where consent is used, it must be freely given, specific, informed and unambiguous, and explicit where required. Compass records what was agreed, when, how and which information was provided. Withdrawal must be as easy as giving consent and does not cause an unfair disadvantage. Staff must explain any processing that continues under a separate lawful basis and must not retrospectively switch basis to evade withdrawal.

### 6.1 Special Category Data

Where Compass processes health, disability, racial or ethnic origin, religious belief, sexual orientation or other special category information, it will identify both an Article 6 lawful basis and an Article 9 condition before processing. Where a UK Schedule 1 condition is relied upon, Compass will also meet the applicable safeguards and maintain an Appropriate Policy Document where required.

### 6.2 Criminal Offence Data

Information about alleged or confirmed offences, police involvement, youth justice, court proceedings or related security measures will be processed only where Compass has an Article 6 lawful basis and either official authority or a specific condition under Schedule 1 of the Data Protection Act 2018. Access and sharing will be strictly controlled and documented.

### 6.3 Biometric identity verification in recruitment

Compass may use online document and biometric identity verification only after the Director has approved the documented arrangements below. These requirements must be met before biometric checks begin or resume; this policy does not itself

establish a lawful basis or confirm that the checks have been completed. A biometric result supports, and does not replace, the other required recruitment checks.

Before use, Compass will assess the actual verification process, including facial matching, liveness checks, identity documents, images and any biometric templates; identify which parties act as controller or processor; and complete a DPIA addressing necessity, proportionality, accuracy, discrimination, security and less intrusive alternatives. If high residual risk remains, required ICO consultation must be completed before processing.

An Article 6 lawful basis and a separate Article 9 condition must be identified and recorded where biometric data is processed to uniquely identify an applicant. Identity verification or safer recruitment does not, by itself, supply an Article 9 condition. Where explicit consent is relied upon, Compass must offer an effective non-biometric route without unfair disadvantage, provide a genuine choice and record explicit consent separately. If valid consent or another applicable condition cannot be established, biometric processing must not take place.

Applicants receive clear privacy information before the check, explaining the provider, purpose, data collected, processing roles, recipients, overseas access or transfers, retention, the alternative route, withdrawal arrangements where relevant, and how to challenge a result. Compass will complete supplier due diligence and the appropriate written agreement, verify subprocessors and transfer safeguards, and prohibit reuse for unrelated purposes unless separately assessed and lawfully authorised.

Access to verification material must be restricted. Compass will retain the minimum verification outcome and audit evidence needed for recruitment; raw biometric templates, images and identity documents must not be retained merely because the system permits it. Exact retention and deletion periods, including provider copies, must be agreed and recorded before use, with deletion verified appropriately. A failed or uncertain match receives meaningful human review and an opportunity for the applicant to explain or use the approved alternative. Appointment decisions must not be based solely on a biometric score.

## 7. Collection, Transparency and Data Minimisation

Compass will collect information directly from individuals where appropriate and may also receive information from commissioning schools, local authorities, parents or carers, health professionals, social care, police, awarding organisations and other authorised sources. Collection forms and referral processes will request only information reasonably necessary for suitability, safety, education, support, accreditation, administration or legal compliance.

- Ordinary website enquiry forms must not invite detailed EHCP, medical, safeguarding or other highly sensitive learner information.
- Privacy information will be provided when information is collected directly. Where it is obtained from another source, it will be provided within a reasonable period and no later than one month, or earlier at the first communication with the individual or first disclosure to another recipient where required. Any applicable exception must be assessed and recorded, not assumed.
- Privacy information will be concise, accessible and age-appropriate where directed at children.
- A new or materially changed use of personal information will not begin until lawful basis, transparency, necessity, security, retention and sharing have been considered.

Privacy notices identify the legal organisation and contact details, purposes and lawful bases, any legitimate interests, relevant categories and sources, recipients, international transfers and safeguards, retention periods or criteria, applicable rights and consent withdrawal, and routes for complaints to Compass and the ICO. They also explain mandatory information and consequences where applicable, and any relevant automated decision-making. Notices are reviewed when processing changes and made accessible to learners and families.

## 8. Data Protection by Design, Risk and DPIAs

Data protection will be integrated into the design of services, systems, forms, contracts and working practices. Compass will use proportionate measures including minimisation, role-based access, pseudonymisation or anonymisation where appropriate, secure defaults, access logging and clear retention settings.

A DPIA screening assessment will be completed for new or materially changed processing. A full DPIA will be completed before processing that is likely to create a high risk to individuals, including relevant large-scale or particularly intrusive uses of children's, safeguarding, health, criminal-offence or monitoring information. Where Compass acts as processor, it will provide reasonable assistance to the controller's DPIA and implement agreed controls.

Risks will be recorded, assigned to an owner, assessed for likelihood and impact, and reduced, avoided, transferred or formally accepted. High residual risk will be escalated and the ICO consulted where legally required before processing begins.

## 9. Accuracy and Record Quality

Staff must distinguish facts, professional opinions, allegations and information supplied by others.

- Important identity, contact, medical, safeguarding, SEND and emergency information will be checked at appropriate intervals and when circumstances change.
- Confirmed inaccuracies will be corrected without undue delay. A record may be annotated where accuracy is disputed while the matter is reviewed.
- Where inaccurate information has been disclosed, relevant recipients will be informed where required and reasonably practicable.
- Routine data-quality checks and lessons from errors will be recorded and used in staff training.

## 10. Information Security and Confidentiality

Compass will apply security measures appropriate to the sensitivity, volume, context and risk of the information. Detailed operational requirements are contained in the Information Security Policy. Minimum requirements include:

- approved systems, including CPOMS for safeguarding and Microsoft 365 for business email and restricted SharePoint document storage; approved accounts and devices only;
- individual Microsoft 365 accounts for all Compass staff with MFA enabled, strong passwords and individual CPOMS accounts with MFA enabled where supported;
- encryption, automatic screen locking, current software updates, malware protection and secure backups;
- role-based access and regular access reviews, with access removed promptly when a person leaves or changes role;
- restricted safeguarding and medical records, with minimum necessary alerts provided to other staff;
- initials rather than a child's full name in email chains; minimum necessary detail and recipient checking; sensitive records shared through authenticated, restricted links or approved secure channels; any document password sent through a different communication channel;
- no routine use of personal email, personal cloud storage, unapproved messaging services or unencrypted removable media for identifiable learner information;
- no identifiable or pseudonymised learner, safeguarding, health or workforce information entered into public generative AI or unapproved transcription or automation tools; any proposed system must undergo supplier, lawful-basis, transparency, retention and DPIA assessment and written approval before personal information is processed;
- clear-desk, locked storage, secure transport and confidential destruction for paper records;
- immediate reporting of lost devices, compromised credentials, unauthorised access or accidental disclosure.

Personal devices require prior approval and a completed BYOD approval record under the Information Security Policy. Initials remain personal information where the person can be identified from context. Where a full identity is necessary for safe action, it must be conveyed within an approved secure record or verified direct channel. Sharing for urgent safeguarding must not be delayed by uncertainty about routine communication arrangements.

## 11. Sharing, Processors and Subprocessors

Personal information will be shared only where there is a lawful, necessary and proportionate reason. Staff must verify the recipient, share the minimum necessary information, use an appropriate secure method and record significant disclosures where required.

Before appointing a processor, Compass will complete due diligence and put a written contract in place containing the required data protection terms. The supplier will be recorded in the Systems and Recipients Register and reviewed proportionately.

Where Compass is itself acting as processor, it will not engage a subprocessor without the controller's prior specific or general written authorisation. Where general authorisation applies, Compass will notify the controller in advance of intended additions or replacements and allow an opportunity to object. Equivalent data protection obligations will be imposed on each subprocessor, and Compass remains responsible to the controller for the subprocessor's performance.

Processor agreements must describe the processing and require documented instructions, confidentiality, appropriate security, controlled subprocessing, assistance with rights, breaches and DPIAs, return or deletion at contract end subject to law, and information and cooperation for audits. When acting as processor, Compass will tell the controller immediately if an instruction appears to infringe data protection law. Any joint controllership must be assessed separately and covered by a transparent allocation of responsibilities whose essence is made available to individuals.

## 12. International Transfers

Compass will identify whether a supplier, recipient, support function or remote-access arrangement involves a restricted transfer outside the UK. A restricted transfer will be made only where it is covered by UK adequacy regulations, appropriate safeguards such as the UK IDTA or Addendum together with any required transfer risk assessment and supplementary measures, or a valid statutory exception. Transfers and safeguards will be recorded in the Systems and Recipients Register.

## 13. Retention, Return and Secure Disposal

Retention periods and disposal methods are set out in the Compass Learning Data Retention and Secure Disposal Policy and Schedule. Information will not be retained merely because it may be useful in the future.

- Where Compass acts as processor, it will follow the commissioning agreement and documented controller instructions concerning return, retention and deletion.
- Legal holds, safeguarding requirements, complaints, investigations or legal claims may suspend routine destruction.
- Deletion and destruction must include, where applicable, email, Outlook caches, downloads, duplicate copies, shared folders, device storage, paper files and supplier-held information.
- Transfers, returns and significant destruction exercises will be recorded.

## 14. Individual Rights

Depending on the circumstances and lawful basis, individuals may have rights of access, rectification, erasure, restriction, objection, data portability, withdrawal of consent and rights concerning solely automated decisions. Rights are not absolute and exemptions may apply.

- Requests may be made verbally or in writing and do not need to use legal terminology.
- Any staff member receiving a request must forward it immediately to the Data Protection Lead and preserve relevant information.
- Identity or authority will be verified proportionately before information is disclosed or altered.
- Compass will normally respond without undue delay and within one month, subject to any lawful extension or pause permitted by law.
- Where Compass acts as processor, it will notify and assist the relevant controller in accordance with the contract rather than deciding the controller's response unless authorised to do so.
- Responses will be disclosed securely and third-party information, safeguarding risks and applicable exemptions will be considered.
- Detailed steps are contained in the Information Rights and Subject Access Request Procedure.

Children’s information rights belong to the child. Before responding to a parent or representative, Compass considers the child’s understanding and competence, the person’s authority, the child’s wishes and best interests, and any safeguarding or

third-party confidentiality issues. Parental responsibility alone does not create unrestricted access to every record. These decisions are documented and applicable exemptions are considered individually.

Any proposed solely automated decision with a legal or similarly significant effect requires a separate legal and DPIA assessment, appropriate transparency and safeguards under current law, including a route to make representations, obtain human intervention and challenge the decision. Additional restrictions for special category information must be checked. No such system may be introduced through routine approval of an app.

## 15. Personal Data Breaches

Every actual, suspected or near-miss personal data breach must be reported immediately to the Data Protection Lead. Staff must take safe containment action within their competence, preserve evidence and must not conceal the incident or contact affected people, the media or the ICO without authorisation.

- When Compass acts as processor, the relevant controller will be notified without undue delay and within any shorter contractual deadline.
- When Compass acts as controller, the Data Protection Lead will assess whether the ICO must be notified without undue delay and, where feasible, within 72 hours of awareness.
- Affected individuals will be informed without undue delay where the breach is likely to result in a high risk and no relevant exception applies.
- All breaches and near misses, including non-reportable incidents, will be recorded with the decision, reasons, containment and lessons learned.

The detailed response is set out in the Compass Learning Data Breach Procedure.

## 16. Training and Awareness

- All Compass staff read and sign a Staff Acceptable Use Policy during induction.
- All Compass staff will receive data protection and confidentiality training before access to live personal information is granted.
- Refresher training will be provided at least annually and when systems, law, risks or working practices materially change.
- Specialist training will be provided for staff with safeguarding, information security, records management, recruitment, qualification or administrative responsibilities.
- Attendance, completion, understanding and refresher dates will be recorded in the Training Register.
- Key messages will be reinforced through briefings, reminders, supervision and learning from incidents.

## 17. Monitoring, Audit and Management Review

The Data Protection Lead will carry out proportionate monitoring, including reviews of access permissions, information assets, retention and deletion, suppliers, contracts, training, rights requests, breaches and DPIA actions. Significant findings will be reported to the Director, assigned to an owner and tracked to completion.

This policy will be reviewed annually and sooner following material legal guidance, a serious incident, a new system, a new processing purpose, a change in business scale or a significant commissioner requirement. Approval and amendments will be recorded in document control.

## 18. Complaints and Concerns

Individuals can raise a data protection complaint with the Data Protection Lead at info@compass-learning.co.uk, verbally or through another accessible route. Compass will assist anyone who needs help to complain and will provide an accessible electronic route, such as a complaints form. A complaint must not be refused merely because it does not use that form or legal terminology.

Compass acknowledges data protection complaints within 30 days of receipt, or sooner under its Complaints Policy. It takes appropriate steps to investigate without undue delay, keeps the complainant informed of progress and communicates the outcome without undue delay. The response explains findings, remedial action that can be disclosed and the right to complain to the ICO. Complaints, actions and outcomes are recorded securely; information-rights and breach deadlines continue to apply separately. Where the complaint concerns the Data Protection Lead personally, an impartial person will review it. No person is disadvantaged for raising a concern.

### 18.1 Direct marketing and website technologies

Before marketing, Compass checks the lawful basis and the rules under the Privacy and Electronic Communications Regulations (PECR) for the recipient and channel. Named professional contact information remains personal data. Marketing to corporate subscribers and marketing to individuals, sole traders or certain partnerships may be subject to different consent rules; staff must not assume that a publicly available email address permits every marketing use.

Marketing identifies Compass and offers a straightforward opt-out. Objections to processing for direct marketing are honoured and a minimal suppression record is retained so that the person is not re-added. Where consent or a permitted soft opt-in is relied upon, its conditions and evidence are recorded. Purchased or researched contact lists, mailing platforms and tracking features require prior assessment, suitable privacy information and supplier checks.

Website cookies, pixels, local storage and similar technologies are assessed before deployment. Prior consent is obtained where required; any statutory exemption is documented and its conditions met. People receive clear information and appropriate controls to refuse or withdraw consent. Advertising and tracking tools must not be enabled merely because a website platform offers them. Online services likely to be accessed by children are screened for the Children's Code and other applicable requirements before launch or material change.

## 19. Linked Documents and Records

1. Information Asset Register, Controller Register and Systems and Recipients Register;
2. Data Retention and Secure Disposal Policy and Schedule;
3. Data Breach Procedure and Breach Log;
4. Information Security Policy;
5. Information Rights and Subject Access Request Procedure and Request Log;
6. Data Protection Impact Assessment and DPIA Screening Form;
7. DPO Requirement Assessment;
8. Appropriate Policy Document;
9. privacy notices;
10. commissioner data processing agreements and supplier/subprocessor contracts;
11. training, secure transfer, disclosure, access review and destruction records.

The Core Provision DPIA and Data Protection Operational Logs support this policy. The processing registers collectively maintain the required Article 30 records, including purposes, categories of people and data, recipients, transfers, retention and security descriptions, with linked lawful-basis assessments. Processor records cover the relevant controllers and categories of processing. Required records are kept current and available to the ICO on request.

The Director checks that privacy notices, the retention schedule, Appropriate Policy Document, commissioner and supplier agreements and records of actual checks match current practice. Dashboard completion statements are reconciled with underlying evidence. The organisation's legal identity and ICO data protection fee status are verified and kept current where applicable.

## 20. References

**ICO - A guide to the data protection principles:** https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/data-protection-principles/

**ICO - Controllers and processors:** https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/controllers-and-processors/

**ICO - Contracts and liabilities between controllers and processors:** https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/accountability-and-governance/contracts-and-liabilities-between-controllers-and-processors-multi/

**ICO - Data protection impact assessments:** https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/accountability-and-governance/data-protection-impact-assessments-dpias/

**ICO - Individual rights:** https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/individual-rights/

**ICO - International transfers:** https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/international-transfers/

**ICO - Personal data breaches:** https://ico.org.uk/for-organisations/report-a-breach/personal-data-breach/

ICO — Biometric recognition: https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/lawful-basis/biometric-data-guidance-biometric-recognition/

ICO — Data protection complaints: https://ico.org.uk/about-the-ico/media-centre/news-and-blogs/2026/06/new-data-protection-complaints-law-now-in-force/

ICO — Business-to-business marketing: https://ico.org.uk/for-organisations/direct-marketing-and-privacy-and-electronic-communications/business-to-business-marketing/