

Information Rights and Subject Access Request Procedure

Access, rectification, erasure, restriction, portability, objection and related requests

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	Operational procedure for approval

Key rule for staff

A rights request can be made verbally or in writing, to any member of staff, and does not need to mention the UK GDPR or use the words “subject access request”. Forward any possible request to the Data Protection Lead immediately.

1. Purpose and scope

This procedure explains how Compass recognises, records and responds to requests concerning personal information. It applies when Compass is an independent controller and when it must assist a school, academy trust, local authority or other controller as processor.

2. Rights covered

Right	Compass response
Access	Confirm processing, provide the person's personal data and required supplementary information, subject to lawful exemptions and protection of others.
Rectification	Correct inaccurate personal data and complete incomplete data. Mark information as disputed while accuracy is investigated where appropriate.
Erasure	Assess whether information must be erased. The right is not absolute and may not apply where retention is required by law, safeguarding obligations, public-interest functions or legal claims.
Restriction	Store information but prevent further use, except for permitted purposes, while the restriction applies.
Portability	Where applicable, provide personal data supplied by the individual in a structured, commonly used and machine-readable format.
Objection	Assess objections to legitimate-interest or public-task processing and to direct marketing. Direct marketing will stop when a valid objection is received.

Right	Compass response
Automated decision-making	Provide safeguards where solely automated decisions with legal or similarly significant effects are introduced. None are currently planned.
Withdrawal of consent	Stop consent-based processing where consent is withdrawn, unless another lawful basis applies and has been properly identified.

3. Roles

- All staff: recognise possible requests, preserve relevant information and forward the request immediately without promising an outcome.
- Data Protection Lead: log, acknowledge, determine role, verify identity where necessary, coordinate searches, assess exemptions, approve and securely issue the response.
- System and record owners: search their systems and return complete results by the internal deadline.
- Commissioner/controller: lead the response where Compass processes the information solely on its behalf. Compass will assist within the contract timescale.

4. Procedure

Stage	Required action
1. Recognise and forward	Treat any clear request about personal information as a possible rights request. Record the exact wording, date, channel and staff member receiving it.
2. Log and identify role	Enter the request in the Information Rights Log. Determine whether Compass is controller, processor or holds information in both capacities.
3. Notify the controller	Where Compass is processor, notify the relevant controller without undue delay and within the contractual deadline. Do not answer independently unless instructed or legally required.
4. Acknowledge	Acknowledge promptly, explain the process and request proportionate identity evidence or clarification only where reasonably necessary.
5. Calculate the deadline	The normal deadline is without undue delay and within one calendar month. Record the due date and reminders. An extension of up to two further months may be available for complex or numerous requests, with timely explanation.
6. Preserve and search	Suspend routine deletion of relevant material. Search approved systems, Webador mailbox, Outlook/local caches, cloud storage, learner and safeguarding systems, paper files, devices and relevant suppliers.
7. Review and redact	Confirm that material is the requester's personal data, remove duplicates and redact information identifying other people unless disclosure is lawful and reasonable. Consider safeguarding, legal professional privilege, management information and other applicable exemptions.
8. Decide and quality check	Record the decision for each right, obtain specialist advice where needed and complete a second-person check for sensitive or complex disclosures.
9. Respond securely	Use a secure channel appropriate to the sensitivity. Explain the outcome, any information withheld, complaint route and ICO rights.
10. Record and close	Record completion, recipients notified, corrections/deletions/restrictions made and any follow-up actions.

5. Special considerations for learners and families

- Assess whether the learner has sufficient understanding to exercise the right independently. Age alone is not decisive.
- A parent or carer does not automatically have a right to all of a child's personal information. Confirm authority, the learner's wishes and safeguarding implications.
- Use clear, age-appropriate communication and reasonable adjustments.
- Do not disclose information where doing so would create an unjustified safeguarding risk or reveal confidential information about another person, unless lawful and necessary.

6. Rectification and data quality

- Record the source, date and status of important information and distinguish fact, professional opinion and allegation.
- Where accuracy is disputed, annotate the record and restrict use where appropriate while checks are made.
- Notify recipients of a correction, erasure or restriction unless this is impossible or involves disproportionate effort; record the reasoning.
- Complete periodic checks of emergency contacts, medical information, EHCP versions, commissioner contacts and user access.

7. Erasure, restriction and portability controls

- Deletion must include central systems, mailbox copies, Outlook caches, downloads, shared folders, devices and paper where reasonably possible.
- Backup copies may be placed beyond use and deleted through the normal backup cycle where immediate deletion is technically impracticable.
- Restricted records must be clearly flagged and technically or procedurally prevented from ordinary use.
- Portable exports should use a secure CSV, PDF or other commonly used format appropriate to the information and request.

Appendix A – Internal request checklist

Field	Record
Request reference	
Date/time received	
Request wording and channel	
Requester and contact details	
Compass role: controller / processor / both	
Relevant commissioner notified and date	
Identity/authority checks	
Clarification requested and date	
Response deadline	

Field	Record
Systems/people searched	
Deletion suspended/legal hold	
Third-party/redaction review	
Exemptions considered	
Decision approved by	
Response method and date	
Recipients notified of correction/deletion/restriction	
Follow-up actions	

Appendix B – Search locations

- Webador-hosted business mailbox and website form submissions.
- Outlook, including local cached mail, archives and downloaded attachments on authorised devices.
- Learner-management, safeguarding, attendance, qualification and assessment systems.
- Approved cloud storage and shared folders.
- Paper files, locked cabinets, notebooks and secure transfer records.
- Finance, HR, recruitment and supplier systems where relevant.
- Relevant processors or subprocessors, where the contract allows a search or export request.

References and linked guidance

- **ICO: A guide to subject access:** <https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/subject-access-requests/a-guide-to-subject-access/>
- **ICO: Individual rights:** <https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/individual-rights/individual-rights/>