ALMA EDUCATION

Data Protection and Privacy Policy

Approval date:	August 2026
Review date:	August 2027
Version:	1.0
Approved by:	 Melanie Steel, Director of Education
Approved by:	Maxine Wellsbury, Advisory Board

Contents

Statement of Intent
1. Legal Framework and Related Policies
2. Applicable Data
3. Accountability
4. Data Protection Officer
5. Lawful Processing
6. Consent
7. The Right to Be Informed
8. The Right of Access
9. The Right to Rectification
10. The Right to Erasure
11. The Right to Restrict Processing
12. The Right to Data Portability
13. The Right to Object
14. Informing Data Subjects
15. Information Rights Requests
16. Data Protection Complaints
17. Automated Decision-Making and Profiling
18. Data Protection by Design and Default
19. Data Protection Impact Assessments
20. Data Breaches
21. Data Security
22. Safeguarding
23. Publication of Information
24. Photography and Images
25. Procurement and Management of Educational Technology
26. Cloud Computing
27. Use of Generative Artificial Intelligence
28. Data Retention
29. DBS Data
30. Monitoring and Review

Statement of Intent

Alma Education is required to keep and process certain information about its learners, their families, staff, volunteers and external contractors in accordance with its legal obligations under data protection legislation. Alma may, from time to time, need to share personal information about its learners or staff with other organisations, mainly commissioning schools and local authorities, the DfE, and potentially children's social care.

This policy sets out how Alma keeps personal data secure, and ensures all staff are aware of their responsibilities and how Alma complies with the core principles of the UK GDPR. Keeping data secure matters most where it protects the learners, families and staff Alma works with, and clear, practical procedures, backed up in writing, are how Alma delivers that.

Legislation and Statutory Guidance
UK General Data Protection Regulation (UK GDPR)
Data Protection Act 2018
Freedom of Information Act 2000
Data (Use and Access) Act 2025
The Electronic Commerce (EC Directive) Regulations 2002
The Privacy and Electronic Communications (EC Directive) Regulations 2003
The Freedom of Information and Data Protection (Appropriate Limit and Fees) Regulations 2004
Protection of Freedoms Act 2012
Keeping Children Safe in Education (2026)
Non-School AP Voluntary National Standards (Aug 2025)

1. Legal Framework and Related Policies

This policy has due regard to all relevant legislation and statutory guidance, including, but not limited to, the legislation and guidance listed in the table above.

This policy operates in conjunction with the following Alma policies:

- Child Protection and Safeguarding Policy
- Staff Code of Conduct
- Complaints Policy
- Assessment Policy
- SEND Policy

2. Applicable Data

For the purpose of this policy, 'personal data' refers to information that relates to an identifiable, living individual, including information such as an online identifier, for example an IP address. The UK GDPR applies to both automated personal data and to manual filing systems, where personal data is accessible according to specific criteria, as well as to chronologically ordered data and pseudonymised data, for example key-coded.

'Sensitive personal data' is referred to in the UK GDPR as special categories of personal data, and is defined as:

- Genetic data.
- Biometric data.
- Data concerning health.
- Data concerning a person's sex life.
- Data concerning a person's sexual orientation.

Personal data which reveals:

- Racial or ethnic origin.
- Political opinions.
- Religious or philosophical beliefs.
- Trade union membership.

Sensitive personal data does not include data about criminal allegations, proceedings or convictions. In the case of criminal offence data, Alma is only able to process this if it is either under the control of official authority, or authorised by domestic law where the processing is necessary for the purposes of performing or exercising obligations or rights which are imposed or conferred by law in connection with employment, social security, social protection, health or social care purposes, public health, and research.

In accordance with the requirements outlined in the UK GDPR, personal data will be:

- Processed lawfully, fairly and in a transparent manner in relation to individuals.
- Collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall not be considered incompatible with the initial purposes.
- Adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed.
- Accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay.

- Kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods, insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes, subject to implementation of the appropriate technical and organisational measures required by the UK GDPR to safeguard the rights and freedoms of individuals.
- Processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.

The UK GDPR also requires that the controller shall be responsible for, and able to demonstrate, compliance with the above principles.

3. Accountability

Alma will implement appropriate technical and organisational measures to demonstrate that data is processed in line with the principles set out in the UK GDPR and DPA, as amended by the Data (Use and Access) Act 2025, and will provide comprehensive, clear and transparent privacy information. Alma will retain evidence that it complies with these requirements.

Records of activities relating to higher-risk processing will be maintained, such as processing that:

- Are not occasional.
- Could result in a risk to the rights and freedoms of individuals.
- Involve the processing of special categories of data or criminal conviction and offence data.

Internal records of processing activities will include the following:

- Name and details of Alma
- Purpose(s) of the processing
- Description of the categories of individuals and personal data
- Retention schedules
- Categories of recipients of personal data
- Description of technical and organisational security measures
- Details of transfers to third countries, including documentation of the transfer mechanism safeguards in place

Alma will also document other aspects of compliance with the UK GDPR and DPA where this is deemed appropriate, including the following:

- Information required for privacy notices, for example the lawful basis for the processing
- Records of consent
- Controller-processor contracts

- The location of personal data
- Data Protection Impact Assessment (DPIA) reports
- Records of personal data breaches
- Records of data protection complaints, including receipt, acknowledgement, enquiries, progress updates, outcomes and remedial action
- Decisions to rely on recognised legitimate interests, including the applicable condition and why the processing is necessary
- Records of significant decisions based solely on automated processing, including the lawful basis and safeguards applied

Alma will implement measures that meet the principles of data protection by design and data protection by default, such as:

- Minimising the processing of personal data.
- Pseudonymising personal data as soon as possible.
- Ensuring transparency in respect of the functions and processing of personal data.
- Allowing individuals to monitor processing.
- Continuously creating and improving security features.

DPIAs will be used to identify and reduce data protection risks, where appropriate.

4. Data Protection Officer

The Director of Education acts as Alma's Data Protection Officer (DPO), as the central point of contact for all data subjects and others in relation to matters of data protection.

The Director of Education, as DPO, is responsible for:

- Informing and advising Alma and its staff about their obligations to comply with the UK GDPR and other data protection laws.
- Monitoring Alma's compliance with the UK GDPR and other laws, including managing internal data protection activities, advising on DPIAs, conducting internal audits, and providing the required training to staff.
- Cooperating with the ICO and acting as the first point of contact for the ICO and for individuals whose data is being processed.
- Coordinating a proactive and preventative approach to data protection.
- Calculating and evaluating the risks associated with Alma's data processing.
- Having regard to the nature, scope, context and purposes of all data processing.
- Prioritising and focussing on higher-risk activities, for example where special category data is being processed.
- Promoting a culture of privacy awareness across Alma.

- Conducting ad hoc reviews of data practices, ensuring staff understand and are acting in accordance with relevant data protection laws.
- Providing annual training for all staff on the risks, limitations and lawful processing requirements when using generative artificial intelligence technologies.
- Monitoring Alma's handling of data protection complaints and advising on the complaints process.
- Advising on the use of recognised legitimate interests and significant automated decision-making.
- Supporting staff training so that information rights requests and data protection complaints are recognised and referred promptly.

The Advisory Board keeps oversight of how Alma is meeting its data protection obligations, and the Director of Education updates the Advisory Board on data protection matters, including any breach, complaint or significant risk.

Staff will involve the Director of Education, as DPO, in all data protection matters closely and in a timely manner.

5. Lawful Processing

The legal basis for processing data will be identified and documented before processing begins. Under the UK GDPR, as amended by the Data (Use and Access) Act 2025, personal data will be lawfully processed under one or more of the following conditions:

- The consent of the data subject has been obtained
- Processing is necessary for a contract held with the individual, or because they have asked Alma to take specific steps before entering into a contract
- Processing is necessary for compliance with a legal obligation (not including contractual obligations)
- Processing is necessary for the performance of a task conducted in the public interest or in the exercise of official authority vested in the controller
- Processing is necessary for protecting vital interests of a data subject or another person, for example to protect someone's life
- Processing is necessary for the purposes of legitimate interests pursued by the controller or a third party, except where such interests are overridden by the interests, rights or freedoms of the data subject, this condition is not available to processing undertaken by Alma in the performance of its tasks
- Processing is necessary for a recognised legitimate interest specified in Annex 1 to the UK GDPR, namely responding to a request for disclosure for another organisation's public task or official function; national security, public security or defence; emergencies; preventing, detecting or investigating crime; or safeguarding vulnerable individuals

Where Alma relies on recognised legitimate interests, it will identify and document the applicable condition and demonstrate that the processing is necessary. This basis will not be used for significant decisions based solely on automated processing. Where special category or criminal offence data is involved, Alma will also identify an appropriate additional condition.

Where a lawful basis requires processing to be necessary, Alma will ensure that the purpose cannot reasonably be achieved by less intrusive means or by processing less personal data. Consent will not be treated as the default lawful basis where another basis is more appropriate.

Sensitive data will only be processed under the following conditions:

- Explicit consent of the data subject
- Processing conducted by a not-for-profit body with a political, philosophical, religious or trade union aim provided the processing relates only to members or former members, or those who have regular contact with it in connection with those purposes, and provided there is no disclosure to a third party without consent
- Processing relates to personal data manifestly made public by the data subject

Processing is necessary for:

- Conducting obligations under employment, social security or social protection law, or a collective agreement
- Protecting the vital interests of a data subject or another individual where the data subject is physically or legally incapable of giving consent
- The establishment, exercise or defence of legal claims or where courts are acting in their judicial capacity
- Reasons of substantial public interest with a basis in law which is proportionate to the aim pursued and which contains appropriate safeguards
- The purposes of preventative or occupational medicine, for assessing the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment or management of health or social care systems and services with a basis in law
- Reasons of public interest in the area of public health, such as protecting against serious cross-border threats to health or ensuring high standards of healthcare and of medicinal products or medical devices
- Archiving purposes in the public interest, or scientific and historical research purposes or statistical purposes in accordance with a basis in law

When none of the above apply, consent will be obtained from the data subject for the processing of their special category personal data.

Alma will ensure that it has privacy notices established which clearly outline the reasons why it needs to collect personal data. The privacy notice will include the following explicit details:

- Why Alma needs to collect personal data
- The lawful basis relied upon and, where recognised legitimate interests is used, the applicable condition
- What Alma plans to do with the personal data
- How long Alma will keep the personal data
- Whether Alma will share the personal data with any external organisations

The privacy notice will be clear and accessible to data subjects. The privacy notice will also be reviewed by the Director of Education, as DPO, at least annually and whenever significant changes are made to how Alma processes the data that it collects.

Alma will ensure that any families, learners and staff whose personal data is included will be notified of any significant changes to the privacy notice or the way in which Alma processes the data.

For personal data to be processed fairly, data subjects must be made aware:

- That the personal data is being processed.
- Why the personal data is being processed.
- What the lawful basis is for that processing.
- Whether the personal data will be shared, and if so, with whom.
- The existence of the data subject's rights in relation to the processing of that personal data.
- The right to make a data protection complaint to Alma and to complain to the ICO in relation to the processing.

Alma has privacy notices for the following groups, which outline the information above that is specific to them:

- Prospective employees
- Learners and their families
- Alma's workforce
- Third parties
- Advisory Board members
- Volunteers

There may be circumstances where it is considered necessary to process personal data or special category personal data in order to protect the vital interests of a data subject. This may include medical emergencies where it is not possible for the data subject to give consent to the processing. In such circumstances, the Director of Education, as DPO, will be consulted and a decision made only after seeking further clarification.

Where Alma relies on:

- 'Performance of contract' to process a child's data, Alma considers the child's competence to understand what they are agreeing to, and to enter into a contract.
- 'Legitimate interests' to process a child's data, Alma takes responsibility for identifying the risks and consequences of the processing and puts age-appropriate safeguards in place.
- 'Recognised legitimate interests' to process a child's data, Alma identifies the applicable condition, demonstrates necessity, and puts age-appropriate safeguards in place.
- Consent to process a child's data, Alma ensures that the requirements outlined in section 6 are met, and does not exploit any imbalance of power in the relationship between Alma and the child.

6. Consent

Consent must be a positive indication expressly confirmed in words. It cannot be inferred from silence, inactivity, a positive action without words or pre-ticked boxes. Consent will only be accepted where it is freely given, specific, informed and an unambiguous indication of the individual's wishes. Consent can be withdrawn by the individual at any time.

Where consent is given, a record will be kept documenting how and when consent was given, and what the data subject was told.

Alma ensures that consent mechanisms meet the standards of the UK GDPR. Where the standard of consent cannot be met, an alternative legal basis for processing the data must be found, or the processing must cease.

When learners and staff join Alma, the staff member or learner's parent or carer will be required to complete a consent form for personal data use. This consent form covers the taking and use of photographs and videos, among other things. Where appropriate, third parties may also be required to complete a consent form.

Where Alma opts to provide an online service directly to a child, the child is aged 13 or over, and the consent meets the requirements outlined above, Alma obtains consent directly from that child; otherwise, consent is obtained from whoever holds parental responsibility for the child, except where the processing is related to preventative or counselling services offered directly to children. In all other instances, an appropriate age of consent is considered by Alma on a case-by-case basis, taking into account the requirements outlined above.

7. The Right to Be Informed

Adults and children have the same right to be informed about how Alma uses their data. The privacy notices supplied to individuals, including children, in regard to the processing of their personal data will be written in clear, plain, age-appropriate language, which is concise, transparent, easily accessible and free of charge.

In relation to data obtained both directly from the data subject and not obtained directly from the data subject, the following information will be supplied within the privacy notice:

- The identity and contact details of the controller, and the Director of Education, as DPO
- The purpose of, and the lawful basis for, processing the data
- The legitimate interests of the controller or third party
- Where recognised legitimate interests is relied upon, the applicable recognised legitimate interest condition
- Any recipient or categories of recipients of the personal data
- Details of transfers to third countries and the safeguards in place
- The retention period or criteria used to determine the retention period
- The existence of the data subject's rights, including the right to withdraw consent at any time, to make a data protection complaint to Alma, and to lodge a complaint with the ICO
- The existence of automated decision-making, including profiling, how decisions are made, the significance of the process and the consequences

Where data is obtained directly from the data subject, information regarding whether the provision of personal data is part of a statutory or contractual requirement, as well as any possible consequences of failing to provide the personal data, will be provided at the time the data is obtained.

Where data is not obtained directly from the data subject, information regarding the categories of personal data that Alma holds, the source that the personal data originates from and whether it came from publicly accessible sources, will be provided:

- Within one month of having obtained the data.
- If disclosure to another recipient is envisaged, at the latest, before the data are disclosed.
- If the data are used to communicate with the individual, at the latest, when the first communication takes place.

8. The Right of Access

Individuals, including children, have the right to obtain a copy of their personal data as well as other supplementary information, including confirmation that their data is being processed, and the right to submit a subject access request (SAR) to gain access to their personal data in order to verify the lawfulness of the processing. Alma will verify the identity of the person making the request before any information is supplied.

Alma will make a reasonable and proportionate search for the requested personal data. It is not required to undertake searches that would be unreasonable or disproportionate in light of the importance of providing access to the information.

A copy of the information will be supplied to the individual free of charge; however, Alma may impose a reasonable fee to cover the administrative costs of complying with requests that are manifestly unfounded or excessive or if an individual requests further copies of the same information. All fees will be based on the administrative cost of providing the information.

Where a SAR has been made electronically, the information will be provided in a commonly used electronic format.

Where a SAR has been made for information held about a child, Alma will evaluate whether the child is capable of fully understanding their rights. If Alma determines the child can understand their rights, it will respond directly to the child.

Alma will respond without undue delay and at the latest within one month of receiving the request. Where Alma reasonably requires information to confirm the requester's identity, evidence that a third party is authorised to act, or payment of a permitted fee, the response period will begin when that information, evidence or fee is received. The period may be extended by up to two further months where necessary because the request is complex or the individual has made a number of requests. The individual will be informed of any extension and the reasons within the initial one-month period.

Where a request is manifestly unfounded or excessive, Alma holds the right to refuse to respond to the request. The individual will be informed of this decision and the reasoning behind it, as well as their right to complain to the supervisory authority and to a judicial remedy, within one month of the refusal.

Alma will ensure that information released in response to a SAR does not disclose personal data of another individual. If responding to the SAR in the usual way would disclose such data, Alma will:

- Omit certain elements from the response if another individual's personal data would be disclosed otherwise.
- Reject requests that cannot be fulfilled without disclosing another individual's personal data unless that individual consents or it is reasonable to comply without consent.
- Explain to the individual who made the SAR why their request could not be responded to in full.

Alma may ask the individual to clarify the personal data requested only where clarification is reasonably required to provide an effective response. The response period will pause on the day clarification is requested and resume on the day after it is received. Alma will not use clarification to delay a response or require the individual to narrow an otherwise clear request; where the individual does not narrow the request, Alma will still carry out a reasonable and proportionate search.

Alma's response will explain the individual's right to make a data protection complaint to Alma and to complain to the ICO.

9. The Right to Rectification

Individuals, including children, are entitled to have any inaccurate or incomplete personal data rectified.

Requests for rectification will be responded to within one month; this will be extended by two months where the request for rectification is complex.

Requests for rectification will be investigated and resolved, where appropriate, free of charge; however, Alma may impose a reasonable fee to cover the administrative costs of complying with requests that are manifestly unfounded or excessive or if an individual makes multiple requests at once. Alma reserves the right to refuse to process requests for rectification if they are manifestly unfounded or excessive or if exemptions apply.

Alma will take reasonable steps to ensure that data is accurate or is rectified if inaccurate, implementing a proportional response for data that has a significant impact on the individual, for example if significant decisions are made using that data. Alma will restrict processing of the data in question whilst its accuracy is being verified, where possible.

Where the personal data in question has been disclosed to third parties, Alma will inform them of the rectification where possible. Where appropriate, Alma will inform the individual about the third parties that the data has been disclosed to.

Where no action is being taken in response to a request for rectification, or where the request has been investigated and the data has been found to be accurate, Alma will explain the reason for this to the individual and will inform them of their rights to complain to the supervisory authority and to a judicial remedy.

10. The Right to Erasure

Individuals, including children, hold the right to request the deletion or removal of personal data where there is no compelling reason for its continued processing, in the following circumstances:

- Where the personal data is no longer necessary in relation to the purpose for which it was originally collected or processed
- When the individual withdraws their consent where consent was the lawful basis on which the processing of the data relied
- When the individual objects to the processing and there is no overriding legitimate interest for continuing the processing
- The personal data was unlawfully processed
- The personal data is required to be erased in order to comply with a legal obligation

- The personal data is processed in relation to the offer of information society services to a child

Alma will comply with the request for erasure without undue delay and at the latest within one month of receipt of the request.

Alma has the right to refuse a request for erasure where the personal data is being processed for the following reasons:

- To exercise the right of freedom of expression and information
- To comply with a legal obligation for the performance of a public interest task or exercise of official authority
- For public health purposes in the public interest
- For archiving purposes in the public interest, scientific research, historical research or statistical purposes
- The establishment, exercise or defence of legal claims

Alma has the right to refuse a request for erasure for special category data where processing is necessary for:

- Public health purposes in the public interest, for example protecting against serious cross-border threats to health.
- Purposes of preventative or occupational medicine, the working capacity of an employee, medical diagnosis, the provision of health or social care, or the management of health or social care systems or services.

Requests for erasure will be managed free of charge; however, Alma may impose a reasonable fee to cover the administrative costs of complying with requests that are manifestly unfounded or excessive or if an individual makes multiple requests at once.

As a child may not fully understand the risks involved in the processing of data when consent is obtained, special attention will be given to existing situations where a child has given consent to processing and they later request erasure of the data, regardless of age at the time of the request.

Where personal data has been disclosed to third parties, they will be informed about the erasure of the personal data, unless it is impossible or involves disproportionate effort to do so. Where personal data has been made public within an online environment, Alma will inform other organisations who process the personal data to erase links to and copies of the personal data in question.

11. The Right to Restrict Processing

Individuals, including children, have the right to block or suppress Alma's processing of personal data.

Alma will restrict the processing of personal data in the following circumstances:

- Where an individual contests the accuracy of the personal data, processing will be restricted until Alma has verified the accuracy of the data
- Where an individual has objected to the processing and Alma is considering whether their legitimate grounds override those of the individual
- Where processing is unlawful and the individual opposes erasure and requests restriction instead
- Where Alma no longer needs the personal data but the individual requires the data to establish, exercise or defend a legal claim

In the event that processing is restricted, Alma will store the personal data, but not further process it, guaranteeing that just enough information about the individual has been retained to ensure that the restriction is respected in future. Alma will inform individuals when a restriction on processing has been lifted.

Where Alma is restricting the processing of personal data in response to a request, it will make that data inaccessible to others, where possible, for example by temporarily moving the data to another processing system or unpublishing published data.

If the personal data in question has been disclosed to third parties, Alma will inform them about the restriction on the processing of the personal data, unless it is impossible or involves disproportionate effort to do so.

Alma reserves the right to refuse requests for restricting processing if they are manifestly unfounded or excessive or if exemptions apply. The individual will be informed of this decision and the reasoning behind it, as well as their right to complain to the supervisory authority and to a judicial remedy, within one month of the refusal.

12. The Right to Data Portability

Individuals, including children, have the right to obtain and reuse their personal data for their own purposes across different services. The right to data portability only applies in the following cases:

- Where personal data has been provided directly by an individual to a controller
- Where the processing is based on the individual's consent or for the performance of a contract
- When processing is conducted by automated means

Personal data can be easily moved, copied or transferred from one ICT environment to another in a safe and secure manner, without hindrance to usability. Personal data will be provided in a structured, commonly used and machine-readable form. Where feasible, data will be transmitted directly to another organisation at the request of the individual. Alma will not be required to adopt or maintain processing systems which are technically compatible with other organisations.

Alma will provide the information free of charge.

In the event that the personal data concerns more than one individual, Alma will consider whether providing the information would prejudice the rights of any other individual.

Alma will respond to any requests for portability within one month. Where the request is complex, or a number of requests have been received, the period can be extended by two months, ensuring that the individual is informed of the extension and the reasoning behind it within one month of the receipt of the request.

Where no action is being taken in response to a request, Alma will, without delay and at the latest within one month, explain to the individual the reason for this and will inform them of their right to complain to the supervisory authority and to a judicial remedy.

13. The Right to Object

Alma will inform individuals, including children, of their right to object at the first point of communication, and this information will be outlined in the privacy notice. Individuals, including children, have the right to object to:

- Processing based on legitimate interests, recognised legitimate interests, or the performance of a task in the public interest.
- Processing used for direct marketing purposes
- Processing for purposes of scientific or historical research and statistics.

Where personal data is processed for the performance of a public task, legitimate interests, or recognised legitimate interests:

- An individual's grounds for objecting must relate to their particular situation.
- Alma will stop processing the individual's personal data unless the processing is for the establishment, exercise or defence of legal claims, or, where Alma can demonstrate compelling legitimate grounds for the processing, which override the interests, rights and freedoms of the individual.
- Alma will respond to objections proportionally, granting more weight to an individual's objection if the processing of their data is causing them substantial damage or distress.

Where personal data is processed for direct marketing purposes:

- The right to object is absolute and Alma will stop processing personal data for direct marketing purposes as soon as an objection is received.
- Alma cannot refuse an individual's objection regarding data that is being processed for direct marketing purposes.
- Alma will retain only enough information about the individual to ensure that the individual's preference not to receive direct marketing is respected in future.

Where personal data is processed for research purposes:

- The individual must have grounds relating to their particular situation in order to exercise their right to object.
- Where the processing of personal data is necessary for the performance of a public interest task, Alma is not required to comply with an objection to the processing of the data.

Where the processing activity is outlined above but is conducted online, Alma will offer a method for individuals to object online.

The Director of Education, as DPO, will ensure that details are recorded for all objections received, including those made by telephone or in person, and will clarify each objection with the individual making the request to avoid later disputes or misunderstandings. Alma will respond to all objections without undue delay and within one month of receiving the objection; this may be extended by a further two months if the request is complex or repetitive.

Where no action is being taken in response to an objection, Alma will, without delay and at the latest within one month, explain to the individual the reason for this and will inform them of their right to complain to the supervisory authority and to a judicial remedy.

14. Informing Data Subjects

Alma ensures that learners, families and staff whose data is processed by Alma are clearly and explicitly informed about how Alma deals with their personal data. The privacy notice will outline the features and functions of Alma's use of personal data, but the privacy notice itself must be easily accessible to all who wish to view it.

Alma will share its privacy notice with learners and families:

- Through the learner's induction pack when joining Alma.
- At the start of each academic year.
- On Alma's website.

Alma will share its privacy notice with staff through:

- Role application.
- Contract acceptance.
- Regular supervision and appraisal.
- The start of each academic year.

15. Information Rights Requests

As well as the right to rectification, Alma will recognise that its learners have information rights, meaning that they have the right to access or amend any personal information that is held about them. The most common of these are SARs.

A learner can make an information rights request relating to any of the following:

- Changing any inaccurate information that Alma holds about them
- Removing their personal information or record from Alma's systems
- Restricting Alma from processing any data held on the learner
- Stopping Alma from processing any personal data entirely

Alma will respond to information rights requests within the applicable statutory timeframe. SAR response periods will be calculated in accordance with section 8 of this policy, including any permitted pause while reasonably required clarification is awaited.

Alma will train staff to recognise and promptly refer information rights requests and data protection complaints, and to distinguish between them and other service, grievance or safeguarding complaints.

16. Data Protection Complaints

A data protection complaint is an expression of concern that Alma has infringed data protection legislation in the way it has collected, used, shared, stored, secured, retained or otherwise processed personal data, or in the way it has responded to an information rights request. The complainant does not need to use legal terminology, refer to legislation, or use a prescribed form in order to make a data protection complaint.

Alma will provide clear and accessible ways to make a data protection complaint, including an electronic route. Current contact details and the electronic complaints route will be published on Alma's website and in relevant privacy notices. Complaints made verbally, in writing, by email, through social media or through any other Alma channel will be accepted.

Staff who receive a data protection complaint will record it and refer it without delay to the Director of Education, as DPO. Alma will make reasonable adjustments and provide age-appropriate support, where required, and will respond urgently where a complaint raises an immediate safeguarding or security risk.

Alma will:

- Acknowledge receipt of the complaint within 30 days.
- Begin making appropriate enquiries and taking appropriate steps to respond without undue delay; the investigation will not be postponed until the acknowledgement period has expired.
- Keep the complainant informed of the complaint's progress and explain any delay without undue delay.
- Communicate the outcome without undue delay, including the findings, any action taken or proposed, and the right to complain to the ICO.

Where the complainant's identity or a representative's authority is uncertain, Alma will request only the information reasonably necessary to verify it and will do so promptly.

Where the data protection complaint forms part of a wider complaint, grievance or safeguarding matter, the data protection element will be handled under this section and will not be delayed unnecessarily by the wider process.

Where a complaint concerns processing carried out by a processor or joint controller, Alma will coordinate with the relevant organisation under the applicable contract or arrangement while retaining responsibility for its own controller obligations.

Alma will keep a proportionate record of the complaint, acknowledgement, enquiries, evidence, progress updates, outcome and remedial action. The Director of Education, as DPO, will review recurring themes and trends to identify improvements.

Using Alma's complaints process does not affect the individual's right to complain to the ICO or seek a judicial remedy.

17. Automated Decision-Making and Profiling

For the purposes of this policy, a decision is based solely on automated processing where there is no meaningful human involvement in taking the decision. A decision is significant where it produces a legal effect or a similarly significant effect on an individual.

Alma will not make a significant decision based solely on automated processing unless it has identified and documented an appropriate lawful basis, the processing is necessary and proportionate, and the safeguards in this section are in place. Recognised legitimate interests will not be used as the lawful basis for such a decision.

Where a significant solely automated decision is based entirely or partly on special category data, it will only be made where either the decision is based entirely on processing for which the individual has given explicit consent, or both of the following apply: the decision is necessary for entering into or performing a contract, or is required or authorised by law; and the processing meets the substantial public interest condition in Article 9(2)(g) of the UK GDPR.

Alma will not use solely automated processing to make a significant decision about a child.

Alma will conduct a DPIA before introducing significant solely automated decision-making and will assess accuracy, fairness, bias, discrimination, security and the particular risks to children and other vulnerable individuals.

Alma will ensure that safeguards are in place which:

- Provide the individual with information about the decision.
- Enable the individual to make representations about the decision.
- Enable the individual to obtain human intervention by Alma.

- Enable the individual to contest the decision.

Any human review will be meaningful. The reviewer will be suitably qualified, will consider the relevant information independently, and will have authority to change or reject the automated outcome; a nominal approval will not be sufficient.

Alma will not use generative AI or another automated system to determine academic progress, behaviour responses, admissions, safeguarding decisions or staff appraisals without meaningful human involvement.

When automatically processing personal data for profiling purposes, Alma will ensure that appropriate safeguards are in place, including:

- Ensuring processing is fair and transparent by providing meaningful information about the logic involved, as well as the significance and predicted impact.
- Using appropriate mathematical or statistical procedures.
- Implementing appropriate technical and organisational measures to enable inaccuracies to be corrected and minimise the risk of errors.
- Securing personal data in a way that is proportionate to the risk to the interests and rights of the individual and prevents discriminatory effects.

Alma will keep appropriate records of the lawful basis, system logic, personal data used, safeguards applied and any human review.

18. Data Protection by Design and Default

Alma will act in accordance with the UK GDPR by adopting a data protection by design and default approach and implementing technical and organisational measures which demonstrate how Alma has considered and integrated data protection into all aspects of processing activities. In line with the data protection by default approach, Alma will ensure that only data that is necessary to achieve its specific purpose will be processed.

Where Alma provides an online service likely to be accessed by children, it will take account of children's higher protection matters when deciding which technical and organisational measures are appropriate. This includes how best to protect and support child users, the fact that children may be less aware of data protection risks, consequences and rights, and their differing needs at different ages and stages of development. Alma will document how these matters have been considered when designing and operating the service.

Alma will implement a data protection by design and default approach by using a number of methods, including, but not limited to:

- Considering data protection issues as part of the design and implementation of systems, services and practices.

- Making data protection an essential component of the core functionality of processing systems and services.
- Automatically protecting personal data in Alma's ICT systems.
- Implementing basic technical measures within Alma's network and ICT systems to ensure data is kept secure.
- Promoting the identity of the Director of Education, as DPO, as a point of contact.
- Ensuring that documents are written in plain language so individuals can easily understand what is being done with personal data.

19. Data Protection Impact Assessments

DPIAs will be used in certain circumstances to identify the most effective method of complying with Alma's data protection obligations and meeting individuals' expectations of privacy. DPIAs will be conducted prior to the implementation of any generative AI tools where the processing of personal data is involved, particularly if the AI tool automates decision-making, involves profiling, or carries a risk of bias, inaccuracy, or data misuse.

A DPIA will include specific evaluation of the risks associated with AI systems, including fairness, accuracy, accountability, transparency and security, in accordance with the DfE's 'Generative artificial intelligence in education' guidance.

DPIAs will allow Alma to identify and resolve problems at an early stage, thus reducing associated costs and preventing damage from being caused to Alma's reputation which might otherwise occur. A DPIA will be conducted when using new technologies or when the processing is likely to result in a high risk to the rights and freedoms of individuals, and will be used for more than one project, where necessary.

High-risk processing includes, but is not limited to, the following:

- Systematic and extensive processing activities, such as profiling
- Large-scale processing of special categories of data or personal data which is in relation to criminal convictions or offences

Alma will ensure that all DPIAs include the following information:

- A description of the processing operations and the purposes
- An assessment of the necessity and proportionality of the processing in relation to the purpose
- An outline of the risks to individuals
- The measures implemented in order to address risk

Where a DPIA indicates high-risk data processing, Alma will consult the ICO to seek its opinion as to whether the processing operation complies with the UK GDPR.

20. Data Breaches

The term 'personal data breach' refers to a breach of security which has led to the destruction, loss, alteration, unauthorised disclosure of, or access to, personal data. The Director of Education will ensure that all staff are made aware of, and understand, what constitutes a data breach as part of their training.

Effective and robust breach detection, investigation and internal reporting procedures are in place at Alma, which facilitate decision-making in relation to whether the relevant supervisory authority or the public need to be notified.

Report a data breach immediately
Any suspected data breach, a lost device, an email sent to the wrong recipient, unauthorised access, is reported to the Director of Education straight away. Do not wait for the next check-in or supervision session.

Where Alma faces a data security incident, the Director of Education, as DPO, will coordinate an effort to establish whether a personal data breach has occurred, assess the significance of any breach, and take prompt and appropriate steps to address it.

All notifiable breaches will be reported to the relevant supervisory authority within 72 hours of Alma becoming aware of it. Where a breach is likely to result in a risk to the rights and freedoms of individuals, the relevant supervisory authority will be informed, and the individuals concerned will be contacted directly. The risk of the breach having a detrimental effect on the individual, and the need to notify the relevant supervisory authority, will be assessed on a case-by-case basis. In the event that a breach is sufficiently serious, the public will be notified without undue delay.

Within a breach notification to the supervisory authority, the following information will be outlined:

- The nature of the personal data breach, including the categories and approximate number of individuals and records concerned
- The name and contact details of the Director of Education, as DPO
- An explanation of the consequences of the personal data breach
- A description of the proposed measures to be taken to deal with the personal data breach
- Where appropriate, a description of the measures taken to mitigate any possible adverse effects

Where notifying an individual about a breach to their personal data, Alma will provide specific and clear advice to individuals on the steps they can take to protect themselves and their data, where possible and appropriate to do so.

Alma will ensure all facts regarding the breach, the effects of the breach and any decision-making processes and actions taken are documented in line with the UK GDPR accountability principle.

Failure to report a breach when required to do so may result in a fine, as well as a fine for the breach itself.

Alma will work to identify the cause of the breach and assess how a recurrence can be prevented, for example by arranging data protection refresher training where the breach was a result of human error.

21. Data Security

Confidential paper records will be kept securely, with restricted access, and will not be left unattended or in clear view in any session location or shared space.

Digital data is coded, encrypted or password-protected, both on a local device and on a network drive that is regularly backed up off-site. Where digital data is saved on removable storage or a portable device, the device will be kept securely when not in use. Memory sticks will not be used to hold personal information unless they are password-protected and fully encrypted. All electronic devices are password-protected to protect the information on the device in case of theft. Where possible, Alma enables electronic devices to allow the remote blocking or deletion of data in case of theft or loss.

All staff are provided with their own secure login and password, and every device regularly prompts users to change their password.

Emails containing sensitive or confidential information are password-protected if there are unsecure servers between the sender and the recipient. Circular emails to parents and carers are sent blind carbon copy (bcc), so email addresses are not disclosed to other recipients. When sending confidential information, staff will always check that the recipient is correct before sending.

Before sharing data, all staff will ensure:

- They are allowed to share it.
- That adequate security is in place to protect it.
- Who will receive the data has been outlined in a privacy notice.

Where personal information that could be considered private or confidential is carried between session locations, either in electronic or paper format, staff will take extra care to follow the same procedures for security, for example keeping devices under lock and key. The staff member carrying the information accepts full responsibility for its security.

Alma will regularly test, assess and evaluate the effectiveness of any and all measures in place for data security.

Alma takes its duties under the UK GDPR seriously and any unauthorised disclosure may result in disciplinary action.

When disposing of data, paper documents will be shredded and digital storage devices will be physically destroyed when they are no longer required. ICT assets will be disposed of in accordance with the ICO's guidance on the disposal of ICT assets.

Alma holds the right to take the necessary disciplinary action against a staff member if they are believed to be in breach of the above security measures.

22. Safeguarding

Alma understands that the UK GDPR does not prevent or limit the sharing of information for the purposes of keeping children safe.

Alma will identify and document the Article 6 lawful basis for safeguarding processing and, where special category or criminal offence data is involved, the relevant additional condition. Where recognised legitimate interests is relied upon, Alma will document the safeguarding condition and why the processing is necessary.

Never let fear of sharing block a safeguarding concern
Data protection never stops or delays sharing information to keep a learner safe. If you have a safeguarding concern, share it with the DSL. If in doubt, share it anyway and raise the question afterwards.

Alma will ensure that staff have due regard to their ability to share personal information for safeguarding purposes, and that fears about sharing information must not be allowed to obstruct the need to safeguard and protect learners. The Advisory Board will ensure that staff are:

- Confident of the processing conditions which allow them to store and share information for safeguarding purposes, including information which is sensitive and personal, and should be treated as special category personal data.
- Aware that information can be shared without consent where there is good reason to do so, and the sharing of information will enhance the safeguarding of a learner in a timely manner.

Alma will ensure that information pertinent to identify, assess and respond to risks or concerns about the safety of a learner is shared with the relevant individuals or agencies proactively and as soon as is reasonably possible. Where there is doubt over whether safeguarding information is to be shared, especially with other agencies, the DSL will ensure that they record:

- Whether data was shared
- What data was shared

- With whom data was shared
- For what reason data was shared
- Where a decision has been made not to seek consent from the data subject or their parent or carer
- The reason that consent has not been sought, where appropriate

Alma will aim to gain consent to share information where appropriate; however, staff will not endeavour to gain consent if to do so would place a learner at risk. Alma will manage all instances of data sharing for the purposes of keeping a learner safe in line with the Child Protection and Safeguarding Policy.

A learner's personal data will not be provided where the serious harm test is met. Where there is doubt, Alma will seek independent legal advice.

23. Publication of Information

Alma is not a public authority for the purposes of the Freedom of Information Act 2000 and does not operate a Freedom of Information Publication Scheme. Alma nonetheless publishes its policies and key information about its provision on its website, so that families and commissioning bodies can access it easily.

Alma will not publish any personal information, including photos, on its website without the permission of the affected individual. When uploading information to Alma's website, staff are considerate of any metadata or deletions which could be accessed in documents and images on the site.

24. Photography and Images

Alma recognises that photographs and video recordings of identifiable individuals will usually constitute personal data and will therefore be processed in accordance with UK data protection law and the data protection principles.

Alma will use photography and video only where there is a clear and lawful basis for doing so, and will ensure that such use is necessary, proportionate and transparent.

Alma will make clear how photographs and video recordings may be taken and used for its purposes. Where consent is relied upon, Alma will obtain, record and manage that consent appropriately. Where another lawful basis applies, Alma will make this clear and will manage objections and restrictions appropriately, including where safeguarding concerns apply.

Parents and carers may take photographs or videos of their own child during a session for personal or domestic use only, and Alma will make clear where this is not appropriate. Alma will expect any such use to respect the privacy and safeguarding of others. Images or recordings must

not be published, including on social media, where this would include any child other than their own without appropriate permission.

25. Procurement and Management of Educational Technology

For the purposes of this policy, 'EdTech' includes the digital tools and systems Alma uses to support learning, communication, records and administration, for example its safeguarding recording platform, staff portal and any assessment or communication tools. Any new EdTech tool that processes personal data is checked and approved by the Director of Education before it is used, and the DSL is involved where a tool touches safeguarding, online safety or security.

Before approving a new tool, the Director of Education checks:

- What the tool is for, and what personal data it will hold, including whether that includes special category data.
- Why that data is needed, switching off any optional data collection or features Alma doesn't need.
- The lawful basis for using it.
- Who can see the data, and where it is stored.
- Whether Alma or the supplier is responsible for the data at each point.

A DPIA is completed before approval where the tool is likely to carry a high risk to learners' or staff's rights and freedoms, for example a new AI tool, and Alma will not go ahead until that risk has been reduced to an acceptable level.

Before using a new supplier, the Director of Education checks:

- The provider can show it meets UK GDPR requirements and keeps data secure, for example through encryption and secure logins.
- The provider can support Alma in responding to a data request or complaint, and in investigating an incident.
- Where a tool uses AI, the provider can explain how it is moderated and whether personal data is used to train it.

Before personal data is shared with a supplier, Alma confirms in writing what the supplier will do with it, how it will be kept secure, how a breach would be reported, and how data is deleted when no longer needed.

When a new tool is put in place, access is limited to the staff who need it, and only the features Alma actually uses are switched on.

The Director of Education reviews Alma's tools periodically, and whenever a tool changes in a way that affects the data it holds.

When Alma stops using a tool or changes supplier, the Director of Education confirms that Alma's data has been securely returned or deleted.

Alma will not use an EdTech tool where the supplier cannot show it meets these requirements.

26. Cloud Computing

For the purposes of this policy, 'cloud computing' refers to storing and accessing data and programs, such as documents, photos or videos, over the internet, rather than on a device's hard drive. Cloud computing involves Alma accessing a shared pool of ICT services remotely via a private network or the internet.

All staff will be made aware of data protection requirements and how these are impacted by the storing of data in the cloud, including that cloud usage does not prevent data subjects from exercising their data protection rights.

If the cloud service offers an authentication process, each user will have their own account. When assessing any cloud-based or AI-powered service, Alma will ensure that the provider demonstrates UK GDPR compliance, provides explicit guarantees regarding non-retention of input data, and allows Alma to audit or verify compliance where necessary. The use of any cloud services which involve AI processing will be subject to a prior risk assessment and will require a DPIA where personal data is involved. A system will be implemented to allow user accounts to be created, updated, suspended and deleted, and for credentials to be reset if they are forgotten, lost or stolen. Access for staff will be removed when they leave Alma.

All files and personal data will be encrypted before they leave a device and are placed in the cloud, including when the data is in transit between the device and the cloud. A robust encryption key management arrangement will be put in place to maintain protection of the encrypted data. The loss of an encryption key will be reported to the Director of Education, as DPO, immediately; failure to do so could result in accidental access or destruction of personal data and, therefore, a breach of the relevant data protection legislation.

As with files on Alma's own devices, only authorised parties will be able to access files on the cloud. An audit process will be put in place to alert Alma should unauthorised access, deletion or modification occur and ensure ongoing compliance with Alma's policies for the use of cloud computing.

Alma's usage of cloud computing, including the service's security and efficiency, will be assessed and monitored by the Director of Education, as DPO. The Director of Education will also ensure that a contract and data processing agreement are in place with the service provider, confirming compliance with the principles of the UK GDPR and DPA. The agreement will specify the circumstances in which the service provider may access the personal data it processes, such as the provision of support services.

The Director of Education, as DPO, will also:

- Ensure that the service provider has completed a comprehensive and effective self-certification checklist covering data protection in the cloud.
- Ensure that the service provider can delete all copies of personal data within a timescale in line with this policy.
- Confirm that the service provider will remove all copies of data, including back-ups, if requested.
- Find out what will happen to personal data should Alma decide to withdraw from the cloud service in the future.
- Assess the level of risk regarding network connectivity and make an informed decision as to whether Alma is prepared to accept that risk.
- Monitor the use of Alma's cloud service, with any suspicious or inappropriate behaviour of learners, staff or families being reported directly to the Director of Education.

27. Use of Generative Artificial Intelligence

Alma recognises that generative AI technologies involve the processing of extensive datasets and may pose increased risks to data privacy and security.

Generative AI tools used by Alma will comply with data protection legislation and Alma will ensure that providers meet the DfE's 'Generative AI: product safety standards'.

To protect data when using generative AI tools, staff members and learners will:

- Seek advice from the Director of Education, as DPO, as appropriate.
- Check the type of tool being used is approved by Alma.
- Understand how the tool uses personal data and whether this adheres to this policy.
- Acknowledge or reference the use of generative AI in their work.
- Fact-check results to make sure the information is accurate.

Check before using AI with personal data

Never enter a learner's or family's personal information into an AI tool without checking with the Director of Education first. This includes names, addresses, and any information about a learner's needs, behaviour or circumstances.

If personal data is entered into an AI tool, the person doing this will first check with the Director of Education that it is safe and appropriate to do so. To avoid a data breach, personal data will be protected within the tool and not used to further train the AI.

Use of generative AI tools must comply with Alma's Staff Code of Conduct. Individuals must not rely solely on AI-generated outputs without appropriate human oversight and validation.

Any incidents, breaches, or concerns arising from the use of AI tools must be reported immediately to the Director of Education and will be investigated in line with Alma's data breach procedures.

28. Data Retention

Data will not be kept for longer than is necessary. Unrequired data will be deleted as soon as practicable. Some educational records relating to former learners or employees of Alma may be kept for an extended period for legal reasons, but also to enable the provision of references or progress records. Paper documents will be shredded or pulped, and electronic records scrubbed clean or destroyed, once the data should no longer be retained.

29. DBS Data

All data provided by the DBS will be managed in line with data protection legislation; this includes electronic communication. Data provided by the DBS will never be duplicated. Any third parties who access DBS information will be made aware of the data protection legislation, as well as their responsibilities as a data handler.

30. Monitoring and Review

This policy is reviewed annually by the Director of Education and the Advisory Board, or sooner if required by changes in legislation or statutory guidance. Any necessary amendments will be communicated to all staff. This policy was approved by Melanie Steel, Director of Education, in August 2026 and is due for review in August 2027.