

Information Governance, Data Protection and Privacy Policy – August 2026

Contents

Purpose.....	2
Scope.....	2
Principles	2
Roles and Responsibilities.....	3
Data Protection Principles	4
Lawful Basis for Processing Personal Information	4
Special Category Personal Information	4
Collecting and Processing Personal Information.....	5
Storage of Personal Information	5
Information Sharing	6
Individual Rights	7
Confidentiality	7
Records Management and Retention.....	8
Data Security	8
Artificial Intelligence and Digital Technologies	9
Personal Data Breaches	9
Privacy by Design and Data Protection Impact Assessments (DPIAs)	10
Staff Training and Awareness	10
Monitoring and Review.....	11
Appendix 1	12
Appendix 2	14
Appendix 3	15
Appendix 4	16
Appendix 5	17
Appendix 6	18
Appendix 7	19

Purpose

AS2Educate is committed to protecting the privacy, confidentiality and security of personal information entrusted to us by children, young people, families, employees, commissioners and partner agencies. Effective information governance supports safeguarding, promotes trust, enables high-quality educational provision and ensures compliance with the UK General Data Protection Regulation (UK GDPR), the Data Protection Act 2018 and other relevant legislation.

This Policy sets out how AS2Educate collects, uses, stores, shares, retains and disposes of personal information. It also establishes the responsibilities of all staff in ensuring that personal data is processed lawfully, fairly, securely and transparently.

AS2Educate recognises that many of the children and young people accessing Alternative Provision have experienced trauma, adversity or complex life experiences. The inappropriate use or disclosure of personal information has the potential to undermine trust and cause further harm. We are therefore committed to handling all information with sensitivity, respect and professionalism, ensuring that personal information is only accessed and shared where there is a lawful basis and a legitimate need to know.

Scope

This Policy applies to all personal information processed by AS2Educate, regardless of format, including information held electronically, in paper records, photographs, audio recordings, emails and any other medium.

It applies to:

- all employees;
- Directors;
- agency staff;
- volunteers;
- contractors;
- consultants;
- work placement students; and
- any individual acting on behalf of AS2Educate.

Principles

AS2Educate is committed to ensuring that all personal information is:

- processed lawfully, fairly and transparently;
- collected for specified, explicit and legitimate purposes;
- limited to the information that is necessary for those purposes;
- accurate and kept up to date;
- retained only for as long as necessary;
- protected through appropriate organisational and technical security measures;
- shared only where there is a lawful basis or safeguarding requirement to do so; and
- managed in a manner that demonstrates accountability, integrity and public confidence.

All staff are expected to understand their responsibilities for protecting personal information and to process information in accordance with this Policy, associated procedures and applicable legislation.

Protecting personal information is a shared responsibility and forms an integral part of safeguarding, professional practice and the effective operation of AS2Educate.

Roles and Responsibilities

AS2Educate recognises that effective information governance requires clear accountability at every level of the organisation.

Provision Manager (Data Protection Lead)

The Provision Manager acts as AS2Educate's Data Protection Lead and is responsible for overseeing compliance with data protection legislation and this Policy.

Responsibilities include:

- promoting a culture of good information governance;
- overseeing compliance with UK GDPR and the Data Protection Act 2018;
- responding to data protection queries and information rights requests;
- overseeing the management of personal data breaches;
- ensuring appropriate records management and retention arrangements are in place;
- approving Data Protection Impact Assessments (where required);
- liaising with the Information Commissioner's Office (ICO) where necessary; and

Senior Leadership Team

The Senior Leadership Team will:

- promote good information governance across the organisation;
- ensure staff understand and comply with this Policy;
- support the secure management of information within their areas of responsibility;
- ensure information is shared appropriately and lawfully; and
- report data protection concerns or breaches promptly.
- ensuring staff receive appropriate information governance training.

All Staff

Every employee, volunteer, contractor and individual working on behalf of AS2Educate has a responsibility to:

- protect the confidentiality, integrity and availability of personal information;
- access only the information necessary to perform their role;
- process personal information lawfully, fairly and securely;
- comply with all relevant AS2Educate policies and procedures relating to information governance;
- report suspected data breaches, information security incidents or concerns immediately;
- complete mandatory information governance training; and
- seek advice whenever they are unsure about the lawful handling or sharing of personal information.

Failure to comply with this Policy may result in management action, disciplinary action or referral to external agencies where appropriate.

Data Protection Principles

AS2Educate will process all personal information in accordance with the principles set out within the UK General Data Protection Regulation (UK GDPR). These principles underpin all aspects of information governance and ensure that personal information is handled lawfully, fairly and responsibly.

AS2Educate will ensure that personal information is:

- processed lawfully, fairly and transparently;
- collected only for specified, explicit and legitimate purposes;
- adequate, relevant and limited to what is necessary;
- accurate and kept up to date where necessary;
- retained only for as long as required;
- protected through appropriate technical and organisational security measures; and
- processed in a manner that demonstrates accountability and compliance with data protection legislation.

Compliance with these principles forms part of every employee's professional responsibility.

Lawful Basis for Processing Personal Information

AS2Educate will only collect and process personal information where there is a lawful basis to do so under UK GDPR.

Depending on the purpose of processing, this may include:

- consent;
- performance of a contract;
- compliance with a legal obligation;
- protection of vital interests;
- performance of a task carried out in the public interest or in the exercise of official authority; or
- legitimate interests where these are not overridden by the rights and freedoms of the individual.

Where special category personal information is processed, AS2Educate will ensure that an additional lawful condition under the Data Protection Act 2018 is also satisfied.

Personal information will never be collected or used for purposes that are incompatible with those for which it was originally obtained unless required or permitted by law.

Special Category Personal Information

AS2Educate processes special category personal information where it is necessary to provide education, safeguard children and young people, support health and wellbeing, fulfil legal obligations or meet the needs of those accessing our provision.

This may include information relating to:

- physical or mental health;
- special educational needs and disabilities (SEND);
- ethnicity;
- religion or belief;
- biometric information (where applicable);
- safeguarding concerns;
- social care involvement; and
- other sensitive information necessary to support children, young people or employees.

Access to special category personal information will be restricted to individuals with a legitimate professional need to know and will be processed with particular care, sensitivity and confidentiality.

AS2Educate recognises that inappropriate disclosure of sensitive information may cause significant distress and, for some individuals, may retraumatise or undermine trust. Staff must therefore ensure that such information is handled respectfully, proportionately and only where there is a lawful basis for doing so.

Collecting and Processing Personal Information

AS2Educate collects personal information directly from individuals, parents and carers, commissioning Local Authorities, previous educational settings and other agencies where there is a lawful basis to do so.

Information collected will be limited to that which is necessary for the purposes of:

- delivering education and support;
- safeguarding children and young people;
- meeting statutory duties;
- managing employment;
- communicating with parents, carers and professionals;
- maintaining accurate records; and
- supporting the safe and effective operation of the organisation.

Where appropriate, individuals will be informed about:

- what information is being collected;
- why it is needed;
- how it will be used;
- who it may be shared with; and
- their rights under data protection legislation.

This information is provided through AS2Educate's Privacy Notice.

Storage of Personal Information

AS2Educate stores personal information using secure electronic systems and, where necessary, secure paper records.

This includes:

- Learntrek, AS2Educate's Management Information System (MIS), which is used to manage student records, attendance, assessments, safeguarding information, behaviour records, SEND information, educational records and communication relating to pupils.
- AS2Educate's secure Google Workspace, including Shared Drives, Gmail and approved Google Workspace applications, where operational records, student documentation, staff records and organisational information are securely stored.
- Avensure's secure Human Resources system, which is used to manage employee records and Human Resources documentation.

Access to personal information is restricted according to job role and the principle of least privilege. Staff will only have access to the information necessary to carry out their professional responsibilities.

Personnel records relating to employees are stored securely within Google Workspace and Avensure's secure HR system. Access to employee records is restricted to members of the Senior Leadership Team and authorised individuals with Human Resources responsibilities.

Information Sharing

AS2Educate recognises that appropriate information sharing is essential to safeguarding children, supporting education and fulfilling legal responsibilities.

Personal information will only be shared where:

- there is a lawful basis to do so;
- it is necessary to protect a child or another person from harm;
- there is a statutory duty to share information;
- consent has been obtained where required; or
- sharing is otherwise permitted by law.
- external quality assurance organisations and regulators where required.

Information may be shared, where appropriate and where there is a lawful basis, with:

- commissioning Local Authorities;
- schools and educational settings;
- Children's Social Care;
- health services, including CAMHS and NHS providers;
- the Police;
- safeguarding partners;
- the Department for Education;
- awarding organisations, examination boards and certification providers;
- approved vocational education and training providers delivering programmes on behalf of AS2Educate;
- other professionals directly involved in supporting the child or young person; and
- regulatory bodies where required by law.

Only the minimum information necessary for the intended purpose will be shared.

Where there is any uncertainty about whether information should be shared, staff must seek advice from the Provision Manager before disclosing personal information unless an immediate safeguarding concern requires urgent action.

Individual Rights

AS2Educate recognises and respects the rights of individuals under UK GDPR.

Subject to applicable legal exemptions, individuals have the right to:

- be informed about how their personal information is used;
- request access to their personal information;
- request correction of inaccurate personal information;
- request erasure of personal information where applicable;
- request restriction of processing;
- object to certain processing activities;
- request the transfer of personal information where applicable; and
- withdraw consent where processing is based on consent.

Requests relating to individual rights should be made to the Provision Manager, who acts as AS2Educate's Data Protection Lead.

All requests will be managed promptly and in accordance with statutory timescales. Where requests relate to information about children or young people, AS2Educate will consider the rights of the child, their level of understanding, parental responsibility and any safeguarding considerations before responding.

Confidentiality

All employees, volunteers, contractors and individuals acting on behalf of AS2Educate have a professional and legal responsibility to maintain the confidentiality of personal information obtained through the course of their work.

Personal information must only be accessed where it is necessary to carry out professional duties and must only be shared where there is a lawful basis, a legitimate professional need to know, or where disclosure is required to safeguard a child or comply with a legal obligation.

Discussions relating to children, young people, families, colleagues or the organisation must take place only in appropriate professional settings and never in public places or with individuals who do not have a legitimate professional need to know.

Staff must not disclose, discuss or share confidential information with family members, friends or other unauthorised individuals. Unauthorised disclosure of confidential information may constitute a breach of this Policy, the Staff Code of Conduct and data protection legislation and may result in disciplinary action.

Maintaining confidentiality does not prevent staff from sharing information where this is necessary to protect a child or another individual from harm. Safeguarding concerns must

always be managed in accordance with the Safeguarding and Child Protection Policy and relevant statutory guidance.

Records Management and Retention

AS2Educate is committed to maintaining accurate, complete and secure records that support the effective delivery of education, safeguarding, organisational management and compliance with legal and regulatory requirements.

Effective records management is an essential part of safeguarding, accountability and the delivery of high-quality education and support. Records will be created, maintained, stored, retained, archived and securely disposed of in accordance with applicable legislation, statutory guidance and AS2Educate's Records Retention Schedule.

AS2Educate will ensure that personal information is:

- created accurately and maintained in a timely manner;
- stored securely using approved electronic systems, including Google Workspace, Learntrek Management Information System (MIS) and Avenure's Human Resources platform, together with secure paper records where appropriate;
- accessible only to authorised individuals who have a legitimate professional need to know;
- reviewed periodically to ensure it remains accurate, relevant and up to date;
- retained only for as long as necessary in accordance with AS2Educate's Records Retention Schedule; and
- archived or securely destroyed when no longer required.
-

Confidential records must not be destroyed outside the arrangements set out within the Records Retention Schedule.

Where records are subject to safeguarding enquiries, complaints, Subject Access Requests, legal proceedings, insurance claims or regulatory investigations, they will be retained until the matter has been fully concluded and any applicable appeal or limitation periods have expired, regardless of the standard retention period.

All confidential records will be disposed of securely to prevent unauthorised access or disclosure. Where appropriate, the secure disposal of records will be documented to demonstrate compliance with data protection legislation and good information governance practice.

Data Security

AS2Educate will implement appropriate technical and organisational measures to protect personal information from accidental or unlawful loss, destruction, alteration, unauthorised disclosure or access.

AS2Educate uses secure cloud-based systems hosted by approved providers to store and manage personal information. Where personal information is processed or stored using cloud services, AS2Educate ensures that appropriate contractual, organisational and

technical safeguards are in place to protect personal information and comply with UK data protection legislation.

These measures include:

- secure password-protected systems;
- Google Workspace for secure document storage, email and collaboration;
- Learntrek Management Information System (MIS) for student records and educational information;
- Avensure's secure Human Resources platform for employee records;
- role-based access controls to ensure staff only access information required for their role;
- multi-factor authentication where available;
- encrypted devices and storage where appropriate;
- secure disposal of confidential waste;
- regular software updates and security measures;
- appropriate backup and recovery arrangements; and
- staff training in information governance and cyber security.

All staff are responsible for ensuring that information is handled securely at all times and must follow the requirements set out within the Digital Safety, Acceptable Use and Professional Online Conduct Policy.

Artificial Intelligence and Digital Technologies

AS2Educate recognises that artificial intelligence (AI) and other emerging digital technologies may support administrative and educational practice when used appropriately. Staff must ensure that the use of AI is lawful, ethical and proportionate and does not compromise confidentiality, safeguarding or the rights of children, young people or employees.

Personal, confidential or special category information must not be entered into publicly available AI platforms or other digital services unless this has been specifically authorised by AS2Educate and appropriate data protection safeguards are in place.

Any content generated using AI that forms part of a student's educational record or organisational decision-making must be reviewed by an appropriately authorised member of staff before use.

Any use of AI must comply with this Policy, the Digital Safety, Acceptable Use and Professional Online Conduct Policy, and all applicable data protection legislation.

Personal Data Breaches

A personal data breach is any accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal information.

Examples may include:

- sending personal information to the wrong recipient;
- loss or theft of devices containing personal information;

- unauthorised access to confidential records;
- cyber security incidents;
- accidental disclosure of confidential information; or
- inappropriate sharing of personal information.

All suspected or actual personal data breaches must be reported immediately to the Provision Manager, who acts as AS2Educate's Data Protection Lead.

Upon notification, AS2Educate will:

- assess the nature and impact of the breach;
- take immediate steps to contain and minimise any harm;
- investigate the circumstances surrounding the incident;
- determine whether notification to the Information Commissioner's Office (ICO) or affected individuals is required;
- maintain appropriate records of the incident and actions taken; and
- identify and implement any learning to reduce the risk of recurrence.

Staff must not attempt to conceal or resolve a personal data breach without informing the Provision Manager.

Privacy by Design and Data Protection Impact Assessments (DPIAs)

AS2Educate is committed to embedding data protection and privacy considerations into all new projects, systems, processes and ways of working.

Privacy by Design means that privacy and information security are considered at the earliest stages of planning and throughout the lifecycle of any activity involving personal information.

Where a proposed activity is likely to result in a high risk to the rights and freedoms of individuals, AS2Educate will complete a Data Protection Impact Assessment (DPIA) before processing begins.

A DPIA may be required where activities involve:

- introducing new technology or software;
- processing large volumes of personal information;
- processing special category or highly sensitive information;
- new methods of information sharing;
- monitoring or surveillance activities; or
- any activity that presents a significant privacy risk.

The Provision Manager, acting as AS2Educate's Data Protection Lead, is responsible for determining when a DPIA is required and ensuring appropriate actions are taken to minimise identified risks.

Staff Training and Awareness

Protecting personal information is the responsibility of everyone working for or on behalf of AS2Educate.

All staff will receive appropriate information governance training:

- as part of their induction;
- through mandatory periodic refresher training;
- following significant changes to legislation or organisational procedures; and
- where additional role-specific training is required.

Staff are expected to seek advice whenever they are uncertain about the lawful collection, use, storage or sharing of personal information.

Monitoring and Review

The Provision Manager, acting as AS2Educate's Data Protection Lead, is responsible for monitoring compliance with this Policy and promoting good information governance throughout the organisation.

This Policy will be reviewed annually, or sooner where there are changes to legislation, statutory guidance, operational practice or organisational structure.

Appendix 1

Records Retention Schedule

AS2Educate will retain personal information only for as long as necessary to fulfil its statutory, safeguarding, operational and contractual obligations. Records will be securely destroyed when they are no longer required in accordance with this Schedule.

Record Type	Retention Period	Disposal Method
Student educational records	In accordance with current DfE guidance (normally until the pupil reaches age 25 unless longer retention is required)	Secure destruction
Child protection and safeguarding records	In accordance with current safeguarding guidance (normally until the child reaches age 25, or longer where required)	Secure destruction
Attendance registers	3 years after the end of the academic year	Secure destruction
Behaviour records	In accordance with DfE guidance and organisational need	Secure destruction
Medical information	Duration of placement plus appropriate statutory retention period	Secure destruction
SEND and EHCP documentation	In line with DfE guidance and commissioning requirements	Secure destruction
Accident records involving children	Until the child reaches age 21 years and 3 months (or longer if litigation is anticipated)	Secure destruction
Accident records involving staff	Minimum 3 years from the date of the accident (longer where required)	Secure destruction
Staff personnel files	6 years after employment ends	Secure destruction
Recruitment records (unsuccessful applicants)	6 months after recruitment process concludes	Secure destruction
DBS and safer recruitment records	DBS certificates should not normally be retained for more than 6 months. Recruitment decision records retained with personnel file where appropriate.	Secure destruction
Payroll records	6 years plus the current financial year	Secure destruction
Pension records	In accordance with pension legislation	Secure destruction
Complaints records	6 years after closure (longer where safeguarding or legal proceedings apply)	Secure destruction
Subject Access Requests	2 years after closure (HR-related SARs may be retained for up to 7 years where justified)	Secure destruction
Data breach records	Minimum 6 years	Secure destruction

Training records	Duration of employment plus 6 years	Secure destruction
Contracts and procurement records	6 years after expiry of the contract	Secure destruction
Financial records	6 years plus the current financial year	Secure destruction
Visitors' signing-in records	12 months	Secure destruction
CCTV recordings (if applicable)	Normally 30 days unless required for investigation, safeguarding or legal proceedings	Secure deletion

Retention periods may be extended where records are required for safeguarding, litigation, insurance claims, statutory investigations or other legal purposes.

Where records are subject to a Subject Access Request, complaint, investigation or legal proceedings, they will not be destroyed until the matter has been concluded and any applicable appeal periods have expired.

All confidential records will be disposed of securely using confidential shredding or secure electronic deletion to prevent unauthorised access.

Where pupils are commissioned by a Local Authority, AS2Educate will retain records in accordance with statutory requirements, commissioning agreements and safeguarding obligations. Where retention periods differ, the longer applicable period will normally apply.

Appendix 2

Subject Access Request Procedure

Individuals have the right to request access to personal information held about them under UK GDPR.

Requests may be made:

- in writing;
- by email;

Requests should be directed to the Provision Manager, who acts as AS2Educate's Data Protection Lead.

Upon receipt, AS2Educate will:

- acknowledge the request;
- verify the applicant's identity where necessary;
- clarify the scope of the request if required;
- identify all relevant information;
- consider any applicable exemptions;
- respond within one calendar month unless an extension is permitted under UK GDPR; and
- provide information in a clear and accessible format.

Where requests relate to children, AS2Educate will consider:

- the child's age and understanding;
- parental responsibility;
- the child's rights under UK GDPR; and
- any safeguarding considerations.

Where AS2Educate refuses all or part of a request, reasons will be provided together with information about the individual's right to complain to the Information Commissioner's Office.

Appendix 3

Subject Access Request Form

Applicant Details

Name:

Address:

Telephone:

Email:

Relationship to AS2Educate:

- ☐ Student
- ☐ Parent/Carer
- ☐ Employee
- ☐ Former Employee
- ☐ Other

Information Requested

Please describe the information you require.

Preferred Format

- ☐ Email
- ☐ Paper Copy
- ☐ Inspection of Records

Identity Verification

Please provide appropriate identification where requested.

Declaration

I confirm that I am entitled to request this information.

Signature

Date

Appendix 4

Personal Data Breach Procedure

A personal data breach is any accidental or unlawful:

- loss;
- destruction;
- alteration;
- disclosure; or
- unauthorised access

to personal information.

Examples include:

- emailing information to the wrong recipient;
- lost laptop;
- stolen paperwork;
- cyber attack;
- unauthorised disclosure;
- accidental deletion.

Staff Responsibilities

Staff must immediately:

- report the incident to the Provision Manager;
- preserve evidence;
- attempt to contain the breach where safe to do so;
- not delete evidence; and
- cooperate with any investigation.

AS2Educate Response

The Provision Manager will:

- assess the breach;
- contain the incident;
- determine the level of risk;
- notify the ICO where required;
- notify affected individuals where appropriate;
- record the breach;
- identify learning; and
- review procedures.

Appendix 5

Personal Data Breach Report Form Date and Time

Reported By

Nature of Breach

- ☐ Loss
- ☐ Theft
- ☐ Incorrect disclosure
- ☐ Cyber incident
- ☐ Unauthorised access
- ☐ Other

Describe the incident

Personal information involved

People affected

Immediate action taken

Reported to Provision Manager

- ☐ Yes
- ☐ No

ICO Notification Required

- ☐ Yes
- ☐ No

Outcome

Lessons Learned

Manager Signature

Appendix 6

Information Sharing Guidance

AS2Educate recognises that appropriate information sharing is essential to safeguarding children, promoting welfare and supporting effective education.

Information will only be shared where:

- there is a lawful basis;
- there is a safeguarding concern;
- there is a statutory duty;
- consent has been obtained where required; or
- disclosure is otherwise permitted by law.

Information may be shared with:

- commissioning Local Authorities;
- schools and educational settings;
- Children's Social Care;
- NHS services;
- CAMHS;
- Early Help;
- Police;
- awarding organisations;
- examination boards;
- certification providers;
- approved vocational education and training providers;
- safeguarding partners;
- regulatory authorities.
- Staff should always:

Fear of sharing information should never prevent staff from taking appropriate action to safeguard a child.

Appendix 7

Data Protection Impact Assessment (DPIA) Template

Project Name

Project Lead

Purpose

Why is this project required?

Personal Information Processed

Special Category Information?

☐ Yes

☐ No

If yes, specify.

Lawful Basis

Potential Privacy Risks

Safeguards

Is consultation required?

☐ Yes

☐ No

Outcome

☐ Approved

☐ Approved with conditions

☐ Not Approved

Data Protection Lead
Name

Signature

Date

Reviewed by:	Richard Fihosy and Claire Ames
Policy Commencement Date:	02.10.2021
Ratified by:	Provision Manager and DSL
Review:	Annual
Next Review:	Autumn Term 2027
Review Date 08.03.24 Richard Fihosy	Page and Sections Page 1 - Former Director's name was deleted.
Aug 25	Full Policy Review
Aug 26	Full Policy Review and rename