THE ALTERNATIVE SCHOOL GROUP LTD

Data Protection Policy

UK GDPR – Data Protection Act 2018 – Data (Use and Access) Act 2025 – Safeguarding Information Sharing September 2026

This policy should be read with the Safeguarding/Child Protection Policy, Privacy Notices, Records Retention Schedule, Online Safety/Acceptable Use arrangements and Personal Data Breach Procedure.

Author:	**HB**
Date:	**14th September 2026**
To be reviewed:	**July 2027**
Reviewed:	**May ’18; Oct ’19; Feb ’20; June ’21; Sept ’22; Sept ’23; Sept ’24; July ‘25’; Sept ‘26**
Version:	**9**

Note: This policy has been developed and reviewed by The Alternative School Group Limited using internal expertise, professional judgement, current statutory guidance and appropriate digital tools. Final approval and responsibility for the policy rests with The Alternative School Group Limited.

Policy status and scope

© 2026 by The Alternative School Group Ltd. All rights reserved.

Purpose. This policy sets out how The Alternative School Group Ltd (TAS) handles personal information lawfully, fairly, transparently and securely, and how it demonstrates accountability. It applies to personal data in any format and to all staff, pupils, parents/carers, advisory board members, contractors, volunteers and others processing personal data for or on behalf of TAS.

Safeguarding priority. Data protection law does not prevent appropriate information sharing to safeguard children. Where information is relevant to safeguarding or promoting a child's welfare, staff must follow safeguarding procedures promptly and must not allow uncertainty about data protection to cause avoidable delay. The Designated Safeguarding Lead (DSL) and DPO should work together where necessary, but a safeguarding decision must not be delayed simply to obtain DPO advice.

Regulatory context. This policy has been refreshed for the September 2026 position, including the Data (Use and Access) Act 2025 (DUAA), Keeping Children Safe in Education 2026, DfE data protection guidance updated July 2026, the DfE statutory information-sharing guidance updated 10 September 2026, and the September 2026 ISI and Ofsted inspection frameworks/toolkits. Inspection frameworks do not create a separate data-protection regime; they test whether leadership, safeguarding, governance and statutory requirements are implemented effectively in practice.

Contents

1. Aims
2. Legal and regulatory framework
3. Key definitions
4. Data controller and governance
5. Roles and responsibilities
6. Data protection principles and accountability
7. Lawful processing and transparency
8. Children's data and safeguarding information sharing
9. Sharing personal data more generally
10. Data subject rights and subject access requests
11. Data protection complaints
12. Photographs, video, CCTV, filtering and monitoring
13. Artificial intelligence, automated decision-making and EdTech
14. Data protection by design, DPIAs and procurement
15. Security, storage, remote working and access controls
16. Retention, transfer and disposal of records
17. International transfers
18. Personal data breaches
19. Training, assurance and monitoring
20. Related policies and records

Appendix 1 – Personal data breach procedure

Appendix 2 – Safeguarding information-sharing decision framework

© 2026 by The Alternative School Group Ltd. All rights reserved.

1. Aims

TAS aims to protect the rights and freedoms of individuals while enabling the lawful use and sharing of information needed to educate pupils, run the organisation, meet legal duties and safeguard children. We will process only the personal data we need; be clear about what we do with it; keep it accurate and secure; retain it only for as long as justified; respect information rights; and be able to demonstrate compliance.

2. Legal and regulatory framework

This policy is informed by, and must be applied consistently with, the following legislation and statutory/regulatory guidance as applicable to TAS:

- UK General Data Protection Regulation (UK GDPR), as amended;
- Data Protection Act 2018 (DPA 2018), as amended;
- Data (Use and Access) Act 2025 (DUAA) – all data-protection provisions now in force;
- Privacy and Electronic Communications Regulations 2003 (PECR), where applicable;
- Children Act 2004, including section 16LA (Information Sharing Duty) from 30 September 2026 where TAS/personnel are within scope;
- Children's Wellbeing and Schools Act 2026;
- Keeping Children Safe in Education (KCSIE) 2026;
- Working Together to Safeguard Children and the DfE statutory guidance Information sharing to safeguard children and young people, updated 10 September 2026;
- DfE Data protection in schools guidance, updated 9 July 2026, used as sector good practice for independent schools where relevant;
- ICO UK GDPR, data-sharing, children's information, complaints, surveillance and international-transfer guidance;
- Independent School Standards and the ISI inspection framework (September 2026), and Ofsted's September 2026 school inspection materials as a cross-check of safeguarding/governance expectations.

Where legislation, statutory guidance or binding regulatory requirements change, the current legal requirement takes precedence over wording in this policy. The DPO will arrange an earlier review where a material change occurs.

3. Key definitions

Term	Meaning
Personal data	Information relating to an identified or identifiable living person.
Special category data	Personal data revealing racial or ethnic origin, political opinions, religious/philosophical beliefs, trade union membership, genetic data, biometric data used for unique identification, health data, or data about sex life or sexual orientation.
Criminal offence data	Personal data relating to criminal convictions/offences or related security measures.
Processing	Any operation performed on personal data, including collection, recording, organisation, storage, alteration, retrieval, use, disclosure, sharing, restriction, deletion or destruction.
Controller	The person or organisation determining the purposes and means of processing.
Processor	A person or organisation processing personal data on a controller's behalf.
Personal data breach	A security breach leading to accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data.
DPIA	Data Protection Impact Assessment: a documented assessment of privacy risks and safeguards, required where processing is likely to result in high risk.

© 2026 by The Alternative School Group Ltd. All rights reserved.

Term	Meaning
Safeguarding information	Information relevant to protecting a child from maltreatment, preventing impairment of health/development, ensuring safe and effective care, or otherwise safeguarding/promoting welfare.

4. Data Controller and Governance

The Alternative School Group Ltd is the data controller for personal data where it determines why and how that data is processed. TAS will maintain its ICO registration/data protection fee position as legally required and will maintain appropriate records of processing activities, privacy notices, contracts, data-sharing arrangements, DPIAs and retention controls.

Governance oversight sits with the Advisory Board. The Board will receive sufficient assurance to understand significant data-protection risks, safeguarding information-sharing arrangements, material breaches, complaints trends, training and audit findings.

5. Roles and responsibilities

5.1 Advisory Board

- Provides oversight and challenge on data protection and information governance.
- Approves this policy and receives periodic assurance from the DPO/senior leadership.
- Ensures safeguarding and data-protection responsibilities are appropriately resourced and integrated.

5.2 Data Protection Officer (DPO)

The DPO advises TAS, monitors compliance, supports DPIAs, provides/coordinates training, advises on breaches and complaints, and acts as a contact point for data subjects and the ICO. The DPO must be involved appropriately and in a timely manner in issues relating to personal-data protection and must be able to perform the role independently.

5.3 Data Protection Lead (DPL)

The DPL is an internal point of contact, to foster a culture of data privacy, champion best practices and handle immediate SAR's, FOI requests or local data breaches. They do not make final legal judgements, instead they implement recommendations and consult the DPO whenever complex issues arise. The DPL for TAS is Heather B and contact is heather@thealternativeschool.co.uk

5.4 Headteacher and Senior Leaders

- Implement this policy operationally and support a culture of secure, proportionate information handling.
- Ensure staff follow safeguarding information-sharing procedures and that concerns are escalated to the DSL without delay.
- Ensure new systems, suppliers and high-risk processing are referred for DPO/DPIA review before implementation, where required.

5.5 Designated Safeguarding Lead (DSL)

- Leads decisions about safeguarding information sharing in accordance with KCSIE, Working Together To Safeguard Children and current statutory information-sharing guidance.
- Records significant sharing decisions, including what was shared, with whom, why, the lawful basis/condition where relevant, whether consent was sought or relied upon, and any decision not to share.
- Consults the DPO where data-protection advice is useful, without delaying action needed to protect a child.

5.6 All staff, contractors and volunteers

- Only access and use personal data needed for authorised duties.

© 2026 by The Alternative School Group Ltd. All rights reserved.

- Follow confidentiality, security, acceptable-use, safeguarding and records-management requirements.
- Immediately report suspected data breaches, loss, misdirection, inappropriate access, cyber incidents or unsafe AI use.
- Forward rights requests and data-protection complaints promptly to the DPO, regardless of the form in which they are received.
- Do not obstruct appropriate safeguarding information sharing because consent is absent where another lawful basis/condition applies.

6. Data protection principles and accountability

TAS will comply with the UK GDPR principles. Personal data must be processed lawfully, fairly and transparently; collected for specified, explicit and legitimate purposes; adequate, relevant and limited to what is necessary; accurate and kept up to date where necessary; kept no longer than necessary; and processed with appropriate security. TAS is responsible for, and must be able to demonstrate, compliance with these principles.

Accountability measures include governance oversight, documented processing records, privacy notices, retention schedules, staff training, access controls, processor contracts, DPIAs, data-sharing agreements where appropriate, breach and complaint logs, and periodic review/audit.

7. Lawful processing and transparency

7.1 Lawful bases

For each processing purpose TAS will identify an appropriate Article 6 UK GDPR lawful basis. These include consent, contract, legal obligation, vital interests, public task/official authority where applicable, and legitimate interests. Where relevant under the DUAA, TAS may rely on a recognised legitimate interest specified in law. The appropriate basis is determined for the activity; consent is not automatically required merely because personal data is being used or shared.

7.2 Special category and criminal offence data

Special category data requires both an Article 6 lawful basis and an Article 9 condition. Criminal offence data requires an Article 6 lawful basis and an applicable condition under the DPA 2018. Where a DPA 2018 condition requires an Appropriate Policy Document, TAS will maintain one and meet the associated safeguards.

7.3 Consent

Where consent is relied upon it must be freely given, specific, informed, unambiguous and evidenced; explicit consent will be obtained where required. Consent can be withdrawn. TAS will not seek consent where the processing is in fact necessary under another more appropriate lawful basis, particularly where seeking consent could create a misleading impression that a statutory or safeguarding activity is optional.

7.4 Privacy information

TAS will provide clear, accessible and age-appropriate privacy information. Privacy notices will explain the purposes, lawful bases, categories of information, recipients, retention, rights, DPO/ICO contact routes, international transfers where relevant, and significant automated decision-making. Notices will be reviewed at least annually and when processing materially changes. Where filtering and monitoring is used, privacy information will explain what is monitored, why, who can access reports/alerts and how long the information is retained.

© 2026 by The Alternative School Group Ltd. All rights reserved.

8. Children's Data and Safeguarding Information Sharing

8.1 Core rule

The safety and welfare of the child is central. Data protection law provides a framework for lawful information sharing and is not a barrier to safeguarding. Staff should be open and transparent about information sharing where it is safe and appropriate to do so, but must not tell a child, parent or other person if doing so could increase risk, prejudice an investigation, undermine safeguarding action or otherwise be inappropriate.

8.2 Consent and Safeguarding

Consent is not usually required to share personal information for safeguarding where another lawful basis applies. Staff must not promise confidentiality that would prevent necessary safeguarding disclosure. The DSL will decide what needs to be shared, applying necessity, relevance, proportionality, accuracy, timeliness and security.

8.3 New Information Sharing Duty – Section 16LA Children Act 2004

The DfE statutory guidance updated on 10 September 2026 reflects the Information Sharing Duty in section 16LA of the Children Act 2004, inserted by the Children's Wellbeing and Schools Act 2026. The duty comes into force on 30 September 2026 and applies in England to the persons within section 16LA(4): persons/bodies listed in section 11(1) of the Children Act 2004; designated childcare or education agencies for section 16E; and persons providing relevant safeguarding/welfare services pursuant to arrangements made by those persons/bodies. TAS will confirm and document the basis on which each relevant TAS provision or service falls within scope, including any designation or commissioning/service arrangement.

Where TAS, or a person acting for TAS, is a relevant person within section 16LA(4), and holds information about a child (or information about another individual that relates to that child) which it considers relevant to safeguarding or promoting the child's welfare, it must ensure that the information is disclosed to another relevant person if, and only so far as, it considers that the disclosure may facilitate the recipient's relevant safeguarding/welfare functions or the relevant services it provides. The duty is proactive and also applies where a relevant person receives a request for the information from another relevant person. A request does not remove the need to decide what information falls within the statutory test.

The statutory duty does not apply where the relevant person considers that disclosure would be more detrimental to the child than not disclosing the information. This is a child-centred professional judgement and must not be confused with a general preference for confidentiality, lack of consent or anxiety about data protection. Where appropriate, staff should consider whether risk can be reduced by limiting, sanitising or restricting the information disclosed. Decisions to withhold or limit information must be clearly recorded and reviewed. In discharging the duty, TAS must have regard to the Secretary of State's statutory guidance. A disclosure made under section 16LA does not breach an obligation of confidence owed by the person making the disclosure, although all other applicable legal and security requirements must still be observed.

Where section 16LA does not directly apply to a particular TAS activity or proposed recipient, staff must still consider other safeguarding powers/duties and the applicable data-protection framework. The September 2026 statutory guidance remains important safeguarding practice. Uncertainty about scope should be escalated promptly to the DSL/DPO and, where appropriate, the local safeguarding partners; necessary immediate safeguarding action must not be delayed.

8.4 Recording Safeguarding Sharing Decisions

- Record the child/individual concerned and the safeguarding purpose.
- Record what information was shared or requested, with whom, when and by whom.

© 2026 by The Alternative School Group Ltd. All rights reserved.

- Record why sharing was necessary/relevant and the lawful basis and additional condition where applicable.
- Record whether the section 16LA duty applies, where relevant, and any local information-sharing agreement used.
- Record whether the person was informed or consent was considered, and why it was or was not appropriate to seek/rely on consent.
- Record any decision not to share, including the reasons.
- Use secure methods and verify the recipient where practicable.

8.5 Transfer of safeguarding records

When a pupil leaves, the DSL will ensure safeguarding/child-protection records are transferred securely and promptly in accordance with KCSIE 2026 and current safeguarding guidance, separately from the main pupil file where appropriate, with confirmation of receipt. Relevant information needed to support the child should be shared in time for the receiving setting to act.

9. Sharing personal data more generally

TAS may share personal data where there is a lawful basis and the sharing is fair, necessary and proportionate. This may include sharing with local authorities, DfE, safeguarding partners, police, health bodies, regulators/inspectors, professional advisers, insurers, examination bodies, education providers and contracted service providers, depending on purpose and legal basis.

Before routine or systematic sharing, TAS will consider whether a written data-sharing agreement is appropriate. Agreements should identify the parties, purposes, data, lawful bases/conditions, roles, security, retention, individual rights, incident handling and review arrangements. Processor relationships must be governed by compliant contracts and appropriate due diligence.

Emergency information may be shared where necessary to protect vital interests or where another lawful basis applies. Only the minimum information reasonably needed should be shared, unless the law requires otherwise.

10. Data subject rights and subject access requests

Individuals, including children, have information rights under data-protection law, subject to statutory conditions and exemptions. These include rights to be informed, access, rectification, erasure, restriction, portability in applicable cases, objection, and safeguards concerning solely automated decisions.

10.1 Subject access requests (SARs)

A SAR can be made verbally or in writing and does not need to use the words “subject access request”. Any member of staff receiving a request must forward it immediately to the DPL. TAS will respond without undue delay and normally within one month, subject to lawful extensions. Identity will be verified proportionately where necessary. Searches must be reasonable and proportionate, and third-party information and applicable exemptions will be considered before disclosure.

10.2 Children and requests made by parents/carers

A child’s personal data belongs to the child. A parent/carer does not automatically exercise the child’s UK GDPR rights. TAS will assess the child’s competence, the requester’s authority, the child’s wishes and best interests, and any relevant exemptions on a case-by-case basis. A parent may make a request on behalf of a child where authorised or where the child is not competent to exercise the right independently.

10.3 Educational records

The statutory parental right of access under the Education (Pupil Information) (England) Regulations 2005 is not treated by this policy as an automatic right in an independent school. Requests for personal data will be considered under UK GDPR/DPA 2018 rights and any other legal, contractual or safeguarding obligations that apply. TAS may provide appropriate educational information to

© 2026 by The Alternative School Group Ltd. All rights reserved.

parents/carers in the ordinary course of education, subject to the child's rights, safeguarding and confidentiality.

11. Data protection complaints

TAS will provide a clear route for people to complain about how their personal data has been handled. Complaints may be made through any published data-protection complaints route. Staff receiving a complaint must forward it promptly.

In line with the DUAA complaint-handling requirements, TAS will acknowledge a data-protection complaint within 30 days of receipt; take appropriate steps to investigate without undue delay; keep the complainant appropriately informed; and communicate the outcome without undue delay. TAS will keep a record of the complaint, enquiries, evidence, decision, response and any remedial action. Individuals will be told of their right to complain to the ICO.

12. Photographs, video, CCTV, filtering and monitoring

12.1 Photographs and video

TAS will identify the purpose and lawful basis for taking and using photographs/video. Consent will be used where appropriate, particularly for optional marketing/promotional uses, and can be withdrawn for future use. Safeguarding considerations, children's wishes and privacy expectations will be respected. TAS will avoid unnecessary identification and will apply secure storage, access and retention controls.

12.2 CCTV

Where CCTV is used, TAS will document its purpose and lawful basis, provide appropriate signage/privacy information, restrict access, set justified retention periods and respond appropriately to access/disclosure requests. A DPIA will be completed where required. CCTV will not be used in areas where people have a high expectation of privacy unless exceptional, lawful and justified.

12.3 Filtering and monitoring

TAS will operate online filtering and monitoring in a lawful, proportionate and transparent manner to support safeguarding. Access to monitoring data will be restricted to authorised, trained staff. Retention and escalation arrangements will be defined, third-party providers will be appropriately governed, and a DPIA will be completed before introducing a new monitoring system or making significant changes where required. Safeguarding alerts will be handled under the school's safeguarding procedures.

13. Artificial intelligence, automated decision-making and EdTech

13.1 AI

Staff and pupils must not enter personal, special category, criminal offence, confidential or safeguarding information into an AI service unless TAS has expressly authorised that service and the intended use following appropriate data-protection, security, contractual and safeguarding assessment. An accidental or unauthorised disclosure to an AI service must be reported immediately as a potential personal data breach.

Before TAS uses AI to process personal data, it will establish purpose and lawful basis, consider data minimisation and transparency, review provider terms and data use, assess international transfers, security and retention, consider children's rights and complete a DPIA where the processing is likely to result in high risk.

© 2026 by The Alternative School Group Ltd. All rights reserved.

13.2 Automated decision-making

The DUAA changed the rules on significant decisions based solely on automated processing. TAS will not use solely automated decision-making with legal or similarly significant effects unless it has a lawful basis and complies with the applicable safeguards. Where required, individuals will be informed of the decision and enabled to make representations, obtain meaningful human intervention and challenge the outcome. Additional restrictions apply to special category data.

13.3 EdTech procurement (Educational Technology)

New EdTech must be assessed before purchase or deployment. TAS will consider controller/processor roles, provider privacy terms, security, access, retention/deletion, sub-processors, AI/model training, advertising/profiling, international transfers, age-appropriate design and exit/data-return arrangements. Procurement convenience must not override data-protection or safeguarding requirements.

14. Data protection by design, DPIAs and procurement

Data protection by design and default must be built into new projects, systems, processes and significant changes. Default settings should use the minimum personal data, access and retention necessary for the purpose.

A DPIA will be completed before high-risk processing begins, including where required for systematic monitoring, innovative technology, large-scale special category data, profiling/automated decisions, or other processing likely to create high risks to rights and freedoms. The DPO will advise. If high residual risk cannot be mitigated, TAS will consider whether prior consultation with the ICO is required.

15. Security, storage, remote working and access controls

TAS will use technical and organisational measures appropriate to the risk. These may include role-based access, strong unique passwords and multi-factor authentication where available/appropriate, encryption, secure configuration, patching, backups, logging, secure email/file-transfer methods, locked storage, clean-desk practices and controlled disposal.

- Personal data must not be accessed or copied merely for convenience or curiosity.
- Personal devices or removable media may only be used where authorised and protected in accordance with TAS requirements.
- Staff must verify recipients before sending sensitive information and use approved secure methods.
- Paper or devices taken off-site must be limited to what is necessary and kept secure.
- Access rights must be reviewed and removed promptly when roles change or people leave.
- Cyber incidents that may involve personal data must be reported immediately to the appropriate internal contact/DPO.

15.1 Working from Home and Remote Access

This subsection applies to home working authorised by TAS following an individual medical-related assessment, including consideration of reasonable adjustments where relevant, and to any other authorised remote access. It does not create a general home-working entitlement. Information about an employee's health or disability used to assess home-working arrangements must be kept confidential, minimised and accessible only to authorised personnel with a genuine need to know.

Where employees are authorised to work from home or another remote location, they must maintain the same standards of data protection, confidentiality and information security as when working on TAS premises.

- **Approved equipment and systems**: Employees must use TAS-approved devices, accounts, applications and secure access arrangements when processing TAS information. Personal

© 2026 by The Alternative School Group Ltd. All rights reserved.

email accounts, personal cloud storage and unauthorised messaging platforms must not be used to store or transfer TAS personal data.

- **Secure internet connections**: Employees must take reasonable steps to ensure their home Wi-Fi is appropriately secured. Public or shared networks must not be used to access confidential information unless suitable TAS-approved security measures are in place.
- **Confidentiality within the home**: Employees must ensure that personal, confidential and safeguarding information cannot be accessed, viewed or overheard by household members, visitors or other unauthorised individuals. Particular care must be taken during telephone calls and online meetings.
- **Device security**: Devices must be locked when unattended and stored securely when not in use. Passwords and authentication credentials must not be shared with others.
- **Paper records and printing**: Printing or taking personal data home must be limited to what is necessary and authorised. Paper records must be securely stored, protected from unauthorised access and returned to TAS for confidential disposal unless another approved secure disposal arrangement is in place.
- **Safeguarding information**: Pupil safeguarding records and other highly sensitive information must only be accessed, processed and shared through approved secure systems and in accordance with TAS safeguarding procedures.
- **Reporting incidents**: Lost or stolen devices, misplaced documents, suspected unauthorised access, accidental disclosure and other potential personal data breaches must be reported immediately in accordance with the TAS Personal Data Breach Procedure.
- **End of home-working arrangements**: Employees must return TAS equipment, documents and records when requested and must not retain unauthorised copies of TAS information.

These requirements should be read alongside the Working from Home Policy, Online Safety and Acceptable Use of ICT Policy, Staff ICT Acceptable Use arrangements, Health and Safety Policy and relevant safeguarding procedures.

16. Retention, transfer and disposal of records

TAS will maintain and follow a records retention schedule. Retention periods must be based on legal requirements, safeguarding needs, limitation periods, operational need and sector guidance. Records will be reviewed periodically and securely destroyed, anonymised or transferred when no longer required. A legal hold, safeguarding need, complaint, investigation or litigation may justify temporary suspension of routine destruction.

Safeguarding and child-protection records require particular care. Their transfer, retention and destruction must follow current safeguarding and records-management guidance and preserve confidentiality, integrity and availability.

17. International transfers

Restricted transfers of personal data outside the UK will only take place where the UK GDPR transfer rules are met. TAS will identify whether an adequacy regulation applies or use an appropriate safeguard such as the UK International Data Transfer Agreement/Addendum where suitable. Where required, TAS will complete the applicable transfer risk assessment/data protection test and document the decision. Supplier cloud locations and onward transfers must be considered during due diligence.

18. Personal data breaches

All actual or suspected personal data breaches must be reported immediately to the DPO. TAS will contain and investigate the incident, assess risk to individuals, document decisions and take remedial action. Where a breach is likely to result in a risk to individuals' rights and freedoms, TAS will notify the ICO without undue delay and, where feasible, within 72 hours of becoming aware. Where a breach is likely to result in a high risk, affected individuals will also be informed without undue delay unless a lawful exception applies.

© 2026 by The Alternative School Group Ltd. All rights reserved.

A breach affecting safeguarding information must also be referred promptly to the DSL so that safeguarding consequences and any need to notify partner agencies can be assessed independently of the data-protection reporting test.

19. Training, assurance and monitoring

All staff and relevant advisory board members will receive data-protection training at induction and refresher training appropriate to their role. Training will include secure handling, breaches, rights requests, complaints, safeguarding information sharing, AI/EdTech and cyber awareness where relevant. DSL/DPO and staff with access to monitoring systems will receive role-specific training.

The DPO will monitor compliance through proportionate audits/reviews, breach and complaint trends, DPIA/processor registers, privacy notice reviews and checks on retention, access and data sharing. This policy will be reviewed at least annually and sooner following material legal, regulatory, safeguarding or technology changes.

20. Related policies and records

- Safeguarding / Child Protection Policy and KCSIE policies
- Privacy notices for pupils/parents, staff and other data subjects
- Records Retention Schedule
- Online Safety and Acceptable Use of ICT policy
- Filtering and Monitoring procedures
- CCTV policy/assessment and signage/privacy information
- AI / Generative AI and EdTech policies
- Complaints Policy and data-protection complaints process
- Personal Data Breach Log and procedure
- Working from Home policy
- Home working and DSE Self Assessment (where relevant)

© 2026 by The Alternative School Group Ltd. All rights reserved.

Appendix 1 – Personal Data Breach Procedure

Stage	Required action
1. Report immediately	Anyone discovering or causing a suspected breach must immediately notify the DPO and, where relevant, IT/security and the DSL. Do not wait to establish all facts.
2. Contain and preserve evidence	Take proportionate steps to stop further disclosure/loss, recover information where possible, preserve logs/evidence and avoid actions that could worsen the incident.
3. Establish facts	Record what happened, when, systems/data involved, categories and approximate numbers of people/records, recipients, security measures, whether data was encrypted, and likely consequences.
4. Risk assessment	Assess severity and likelihood of harm to rights and freedoms, including safeguarding, discrimination, identity/financial harm, confidentiality, distress and vulnerability of children/data subjects.
5. ICO decision	If likely to result in a risk to rights and freedoms, notify the ICO without undue delay and, where feasible, within 72 hours of awareness. If notification is late, record reasons. If not reportable, record the rationale.
6. Individuals	If likely to result in a high risk, notify affected individuals without undue delay unless a statutory exception applies. Use clear language and give practical mitigation advice.
7. Safeguarding	Where safeguarding information or a child's safety may be affected, notify the DSL immediately and consider safeguarding partners/police/other agencies as appropriate. This is separate from the ICO reporting threshold.
8. Review	Record every breach, lessons learned and corrective actions. Review technical, procedural, contractual or training changes needed to prevent recurrence.

Examples include misdirected emails, unauthorised access to safeguarding records, lost devices/paper files, accidental publication, ransomware, compromised accounts, insecure AI uploads, inappropriate CCTV/monitoring disclosure, or a supplier incident affecting TAS data.

© 2026 by The Alternative School Group Ltd. All rights reserved.

Appendix 2 – Safeguarding information-sharing decision framework

This framework supports, but does not replace, professional safeguarding judgement or the statutory guidance. In an emergency, protect the child first and record the decision as soon as practicable.

Question	Action / evidence
1. Is there a safeguarding or welfare purpose?	Identify the concern, risk or welfare purpose and what decision/action the recipient needs to take.
2. Is the information relevant and necessary?	Share enough to achieve the safeguarding purpose; avoid irrelevant detail.
3. Who needs the information?	Confirm the recipient has a safeguarding/welfare role or other lawful need. Verify identity/contact details where practicable.
4. Does section 16LA apply?	From 30 September 2026, confirm whether both the discloser and proposed recipient are relevant persons within section 16LA(4). If the information is relevant to safeguarding or promoting the child's welfare and disclosure may facilitate the recipient's relevant functions/services, the duty requires disclosure unless sharing would be more detrimental to the child than not sharing. The duty also applies to qualifying requests. Have regard to the DfE statutory guidance and applicable local/Tier 1/Tier 2 sharing arrangements.
5. What is the data-protection basis?	Identify Article 6 basis and, for special category/criminal offence data, the relevant additional condition. Consent is not automatically required.
6. Should the person be informed?	Be transparent unless informing them would increase risk, prejudice safeguarding/investigation, be impracticable, or another lawful reason applies.
7. Is the sharing proportionate, accurate and secure?	Check accuracy/context, mark opinion appropriately, use a secure route and limit access.
8. Record the decision	Record what/why/with whom/when, the legal basis/additional condition, the section 16LA scope and statutory test where relevant, any request received, consent/transparency considerations, and any decision to limit or withhold information because disclosure would be more detrimental to the child than non-disclosure. Record review/escalation.

© 2026 by The Alternative School Group Ltd. All rights reserved.

© 2026 by The Alternative School Group Ltd. All rights reserved.