

Data Protection Policy

FASD HUB South West / FASD Informed UK™

Document owner	FASD HUB South West, trading as FASD Informed UK™
Original issue date	10 April 2022
Last reviewed and updated	2 August 2026
Approved	7 August 2026
Next review	1 September 2027, or sooner following a significant data breach, organisational change, or relevant change in law or regulatory guidance
Policy lead	Data Protection Lead, working with the Designated Safeguarding Lead
Copyright	© FASD Informed UK™ / FASD HUB South West 2026. All rights reserved.

Contents

1. Policy statement.....	2
2. Purpose and scope	2
3. Data protection principles	2
4. Governance and responsibilities	2
5. FASD-informed privacy practice.....	2
6. Lawful use of personal information	3
6.1 Special category and criminal offence information.....	3
7. Collection, privacy information and consent.....	3
7.1 Children, decision-making support and representatives	4
8. Sharing and disclosure	4
8.1 Processors and international transfers	5
9. Individual rights	5
10. Accuracy, retention and secure disposal.....	6
11. Security and confidentiality	6
12. Personal data breaches	7
13. Accountability, impact assessment and training.....	7
14. Questions, complaints and review	7
15. Glossary.....	7
16. Legal framework and guidance.....	8

1. Policy statement

FASD HUB South West, trading as FASD Informed UK™, is committed to protecting personal information and respecting the privacy, dignity, choices and rights of everyone whose information we use. We handle personal information lawfully, fairly, transparently and securely under the UK General Data Protection Regulation, the Data Protection Act 2018 and other applicable law.

2. Purpose and scope

This policy applies to directors, employees, workers, volunteers, contractors, students and anyone processing personal information for the organisation. It covers information about participants, children and young people, adults, parents, carers, supporters, staff, volunteers, donors, partners, suppliers and contacts, whether held on paper, digitally, in photographs, recordings, messages, forms, cloud services or other systems. It applies when working from organisational premises, home, outreach settings, hired venues, online and at indoor or outdoor events.

3. Data protection principles

- Lawfulness, fairness and transparency.
- Purpose limitation: information is collected for specified, explicit and legitimate purposes.
- Data minimisation: only information that is adequate, relevant and necessary is used.
- Accuracy: reasonable steps are taken to keep information correct and up to date.
- Storage limitation: identifiable information is retained only as long as necessary.
- Integrity and confidentiality: appropriate technical and organisational security is maintained.
- Accountability: the organisation can demonstrate compliance through records, decisions, training and review.

4. Governance and responsibilities

FASD HUB South West, trading as FASD Informed UK™, is the data controller where it determines why and how personal information is used. As a Community Interest Company, accountability rests with its directors. The directors approve this policy, ensure proportionate resources and oversight, and appoint a suitably competent Data Protection Lead. A statutory Data Protection Officer will be appointed where the legal criteria require one; otherwise the Data Protection Lead coordinates compliance, provides advice and manages contact with the Information Commissioner's Office. Managers are responsible for implementing suitable systems, contracts, privacy information, retention arrangements and staff supervision in their areas. Everyone handling personal information must follow this policy, complete required training, use approved systems, maintain confidentiality and report concerns or breaches immediately.

5. FASD-informed privacy practice

Information about privacy, choices and rights will be provided in clear, concrete and accessible language. We will offer one question or choice at a time where helpful, extra processing time, repetition or rephrasing, written or visual prompts and involvement of a trusted supporter, advocate, parent or carer where appropriate. We will check understanding without relying only on verbal fluency, a “yes”, nod, silence or apparent agreement. Memory, executive functioning, sensory needs, distress, communication differences or fluctuating capacity will not be treated as non-compliance. Support will be individualised and will not create unnecessary barriers to services.

6. Lawful use of personal information

Before processing begins, the organisation will identify and document an appropriate lawful basis for each purpose. Depending on the circumstances, this may include consent, performance of a contract, compliance with a legal obligation, protection of vital interests, performance of a task in the public interest or exercise of official authority, or legitimate interests. Consent is not automatically required and will not be used where it cannot be freely given or withdrawn. When the purpose changes, the lawful basis and privacy information will be reviewed before further use.

6.1 Special category and criminal offence information

Special category information includes racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, genetic information, biometric information used for identification, health information and information about a person’s sex life or sexual orientation. To use it, the organisation must identify both an Article 6 lawful basis and an Article 9 condition, together with any required Data Protection Act 2018 Schedule 1 condition and appropriate policy document. Criminal offence information will be used only where authorised by law and with appropriate safeguards. High-risk processing will be assessed through a data protection impact assessment.

Prenatal alcohol information. Information about possible or confirmed prenatal alcohol exposure is highly confidential health and family information. The organisation will collect, infer, record, use or share it only where this is necessary for a defined purpose, supported by an Article 6 lawful basis and an Article 9 condition, and limited to the minimum detail required. Records will distinguish confirmed information from professional opinion, reported history and uncertainty, identify the source where appropriate, and avoid blame, stigma or unsupported assumptions about a birth parent or family. Access will be restricted to specifically authorised people with a genuine need to know, and disclosure to relatives, professionals, schools, funders or partner organisations will not occur merely because they are involved with the person. Any disclosure must be necessary, proportionate, securely made and recorded, with accessible consent obtained where consent is the appropriate basis. Information may be used or shared without consent only where another lawful basis and legal condition apply, including a safeguarding, vital-interests or legal requirement. Privacy information, retention, correction and rights-request decisions will recognise the potential effect of this information on the privacy, safety, dignity and family relationships of both the person and any identifiable birth parent.

7. Collection, privacy information and consent

At or before collection, people will receive accessible privacy information explaining who is using the information, the purposes, lawful bases, recipients, retention, rights, complaint routes and any international transfer or automated decision-making. We will collect information directly where practicable and record its source where obtained elsewhere. Where consent is the lawful basis, it must be freely given, specific, informed, unambiguous, recorded and as easy to withdraw as to give. Explicit consent will be obtained where required. Withdrawal does not affect processing already carried out lawfully.

7.1 Children, decision-making support and representatives

Children have data protection rights in their own name. The organisation will support each child to understand and exercise those rights in a way appropriate to the child's age, development, communication and circumstances. A person may make a request or receive information for a child only where the organisation is satisfied that the person has parental responsibility, has been lawfully authorised by a person with parental responsibility or by the child where the child is competent to authorise them, or otherwise has a legal power to act, such as a court-appointed guardian or a person authorised by a court order. Foster carers, kinship carers, relatives, advocates, schools, local authorities and professionals will not automatically be treated as entitled to exercise the child's rights or receive the child's information solely because of their role. Identity, authority, the scope of authority and any relevant court order, care order, placement arrangement or restriction will be checked proportionately. Even where authority is established, the organisation will consider the child's competence, views, privacy, best interests and any risk of harm, and will disclose only information that the requester is lawfully entitled to receive. Where parental responsibility is shared, the organisation will not routinely require the agreement of every holder, but will consider objections, disputes, safeguarding concerns and legal restrictions before acting. Safeguarding information may be used or shared without consent where another lawful basis and legal condition apply.

For adults, capacity is decision-specific. The organisation will presume capacity unless there is a lawful reason to assess it and will provide all practicable support before concluding that a person cannot make the particular decision. Where an adult lacks capacity for that decision, any action or decision will follow the applicable legal framework, be in the person's best interests, use the least restrictive option and take account of the person's wishes, feelings, values and relevant views.

Disputed authority. Where authority to act for a child or adult is disputed, unclear or contradicted by another person, the organisation will pause any non-urgent disclosure or decision and refer the matter to the Data Protection Lead and, where safeguarding is relevant, the Designated Safeguarding Lead. The organisation will verify identity and review the available evidence of authority, including parental responsibility, consent, court orders, care or placement arrangements and any stated restrictions. It may seek clarification from the person concerned, other holders of parental responsibility, the relevant local authority, legal advisers or another competent body, but will disclose only the minimum information necessary for that purpose. Urgent action may proceed where required to protect life, prevent serious harm or meet a safeguarding or legal duty. The decision, evidence considered, lawful basis, reasons, information shared and any review or complaint route will be recorded and communicated accessibly to the affected person where lawful and appropriate.

7.2 Children in care and care-experienced people

Where personal information relates to a child in care, a previously looked-after child or another care-experienced person, the organisation will recognise that records may contain particularly sensitive information about health, disability, family relationships, placement history, safeguarding, education and trauma. Information will not be requested or shared simply because a person has care experience. Processing must have a defined purpose, an identified lawful basis and, where relevant, an Article 9 condition. Access will be limited to people who need the information for that purpose, and privacy information will explain how it may be used and shared in a way the person can understand.

8. Sharing and disclosure

Personal information will be shared only where necessary, proportionate and lawful. Before sharing, the organisation will verify the recipient, purpose, lawful basis, authority, minimum information required, security method and any agreement or contract. Information may be shared with local authorities, health or social-care professionals, safeguarding partners, funders, insurers, regulators, emergency services or other organisations where a lawful basis applies. Consent will not be requested or promised where the organisation must disclose information to protect life, prevent serious harm, meet a safeguarding or legal duty, establish or defend legal rights, or comply with a lawful request. Decisions and reasons will be recorded.

8.1 Processors and international transfers

Suppliers processing personal information for the organisation must be subject to due diligence, written data-processing terms, confidentiality, appropriate security, deletion or return requirements, audit rights and controls on sub-processors. Personal information will be transferred outside the UK only where permitted by data protection law, using an adequacy regulation or another valid safeguard and any required transfer risk assessment.

9. Individual rights

- Be informed about how personal information is used.
- Request access to personal information.
- Request correction of inaccurate or incomplete information.
- Request erasure where the law provides.
- Request restriction of processing.
- Receive and reuse information through data portability where applicable.
- Object to processing in certain circumstances.
- Receive safeguards relating to solely automated decisions with legal or similarly significant effects.
- Complain to the organisation and to the Information Commissioner's Office.

Requests may be made verbally or in writing and do not need to use legal terminology. Staff must forward them immediately to the Data Protection Lead. Identity and authority will be checked proportionately. Responses will be provided within the applicable legal time limit, normally one month, unless a lawful extension or exemption applies. Information will be supplied accessibly and ordinarily without charge.

Continuity after transitions. A rights request will remain active if a child changes placement, school, service, address, legal representative or care status, or reaches adulthood while the request is being handled. The Data Protection Lead will retain ownership until a lawful response is completed, recalculate and record any applicable deadline, verify any new contact or authority without unnecessarily repeating checks already completed, and transfer the request record securely to any authorised successor within the organisation. The child or young person and any person lawfully acting for them will be told who is handling the request, how to make contact and whether the transition changes what information may be disclosed. A transition will not be used to restart the statutory response period, close the request or require a fresh request unless the law requires this. Where responsibility moves to another controller, the organisation will explain the limit of its role, respond for information it controls and, where lawful and helpful, provide the correct contact route. Relevant safeguarding restrictions, communication needs, evidence of authority, searches completed, decisions, correspondence and outstanding actions will be recorded so that continuity does not depend on one worker's memory.

10. Accuracy, retention and secure disposal

Information will be accurate, relevant and reviewed when circumstances change. It will be retained under an approved retention schedule based on purpose, legal requirements, safeguarding needs, limitation periods and funder or contractual requirements. When no longer required, paper and digital records will be securely destroyed or anonymised. Devices and storage media will be securely erased before reuse, sale or disposal.

Decisions about deleting, correcting or restricting records concerning care history, safeguarding or family relationships will consider the person's rights, the accuracy and context of the record, legal retention duties and the possible long-term value of information to the person's identity, life story or future access to records. A disputed professional opinion will not automatically be erased; where appropriate, the record will be supplemented with the person's correction, view or contextual statement.

11. Security and confidentiality

Labels and diagnostic shorthand. Personal information must not be disclosed through labels, filenames, folder names, email subject lines, calendar entries, meeting titles, attendee lists, sign-in sheets, badges, envelopes, screen displays or other visible shorthand. Terms such as "FASD", "prenatal alcohol exposure", "care-experienced", "safeguarding", "high risk" or diagnostic abbreviations may be used only where necessary for a defined purpose and visible solely to authorised people with a genuine need to know. Staff will use neutral wording in shared or externally visible contexts, check recipients and access settings before sending or publishing information, and avoid grouping or identifying people by diagnosis, disability, care status or support need. Where a label or code is operationally necessary, its meaning and access will be controlled, it will not contain more information than required, and it will not be reused for an unrelated purpose.

Access will be limited to authorised people with a genuine need to know. Controls will include role-based access, strong authentication, secure configuration, encryption where appropriate, approved devices and services, backups, physical security, clear-desk and secure-transport arrangements, confidentiality commitments, patching, supplier assurance and tested recovery

procedures. Personal information must not be placed in personal email, messaging, storage or artificial-intelligence services unless expressly approved and governed by organisational controls.

12. Personal data breaches

Any loss, destruction, alteration, unauthorised disclosure of or access to personal information, including a near miss, must be reported immediately to the Data Protection Lead. The organisation will contain the incident, preserve evidence, assess risk to people, record facts and decisions, notify affected partners where required and take corrective action. A breach must be reported to the Information Commissioner's Office without undue delay and, where feasible, within 72 hours of awareness if it is likely to risk people's rights and freedoms. People will be informed without undue delay where the breach is likely to create a high risk.

13. Accountability, impact assessment and training

The organisation will maintain proportionate records of processing, lawful-basis decisions, privacy information, consent where used, sharing agreements, processor contracts, retention, rights requests, breaches, training and audits. A data protection impact assessment will be completed before processing likely to create a high risk, including significant new systems, large-scale sensitive information, systematic monitoring, innovative technology or profiling. Data protection by design and default will be built into changes from the outset. Role-appropriate induction and refresher learning are mandatory, and serious or repeated non-compliance may lead to disciplinary or contractual action.

14. Questions, complaints and review

Questions, rights requests and concerns should be directed to the Data Protection Lead through the organisation's published contact route. Complaints will be handled promptly, accessibly and without disadvantage. A person may also complain to the Information Commissioner's Office. This policy will be reviewed by 1 September 2027 and sooner after a significant breach, material change in processing or systems, organisational change, audit finding, or relevant legal or regulatory development.

15. Glossary

- **Personal information:** information relating to an identified or identifiable living person.
- **Processing:** any operation involving personal information, including collection, recording, use, sharing, storage, alteration or deletion.
- **Data controller:** the organisation deciding the purposes and means of processing.
- **Data processor:** a person or organisation processing personal information on a controller's instructions.
- **Data subject:** the person the information relates to.
- **Special category information:** sensitive information receiving additional legal protection.

- **Personal data breach:** a security breach leading to accidental or unlawful destruction, loss, alteration, unauthorised disclosure of or access to personal information.
- **DPIA:** a data protection impact assessment used to identify and reduce high data-protection risks.

16. Legal framework and guidance

- UK General Data Protection Regulation.
- Data Protection Act 2018, as amended.
- Privacy and Electronic Communications Regulations 2003, where applicable.
- Human Rights Act 1998 and common-law duties of confidentiality, where applicable.
- Mental Capacity Act 2005 and safeguarding law and guidance, where relevant to information use and supported decision-making.
- Information Commissioner's Office guidance on data protection principles, lawful bases, special category information, individual rights, children's information, security, data sharing, international transfers, impact assessments and personal data breaches.
- This policy should be read with the organisation's Safeguarding Policy, Equality, Diversity and Inclusion Policy, Health and Safety Policy, confidentiality arrangements, retention schedule, incident response procedure, information-security procedures, consent and media procedures, complaints procedure and processor contracts.

Approved on behalf of FASD HUB South West, trading as FASD Informed UK™, on 7 August 2026.

© FASD Informed UK™ / FASD HUB South West 2026. All rights reserved.