



Data Protection Policy

FACE – Family and Community Enterprise | Registered charity 1179629 | Working as FAM

Head office: Central Buildings, Richmond Terrace, Blackburn, BB1 7AP | Applies at head office and all FAM outreach sites

REFERENCE	VERSION	OWNER	REVIEW
FAM-IG-13	1.0 (September 2026)	Data Protection Lead	Annually

Status: approved by the Board of Trustees on 10 September 2026.

Our commitment

FAM collects and uses personal information about young people, families, volunteers, staff and supporters so that it can deliver safe, good-quality services. We handle that information lawfully, fairly and securely, and we only keep what we need for as long as we need it. Everyone who works or volunteers for the charity shares responsibility for protecting it.

1 Purpose and scope

- 1.1** This policy explains how FACE – Family and Community Enterprise (registered charity 1179629), working as FAM, meets its duties under the UK General Data Protection Regulation (UK GDPR) and the Data Protection Act 2018, as amended by the Data (Use and Access) Act 2025. FAM is the **data controller** for the personal information it holds.
- 1.2** It applies to trustees, staff, volunteers, sessional workers and anyone else who handles personal information on the charity's behalf. It covers paper, electronic and messaging-app records, including those on personal devices used for charity work.
- 1.3** The people whose information we hold include young people aged 11–25, younger children attending holiday clubs, parents and carers, volunteers, staff, job applicants, trustees, donors, funders and partner organisations.

2 The data protection principles

- 2.1** Everything we do with personal information must meet the seven principles in the UK GDPR. In practice this means:

Principle	What it means at FAM
Lawfulness, fairness and	We have a lawful basis for each use and we tell people

Principle	What it means at FAM
transparency	what we do through our Privacy Notice.
Purpose limitation	We use information only for the reasons we collected it, or for compatible reasons.
Data minimisation	Forms ask only for what we need. We do not collect "just in case".
Accuracy	We check details at registration and update them when people tell us of changes.
Storage limitation	We follow the retention schedule in the Records Management and Retention Policy.
Integrity and confidentiality (security)	We lock paper records away, protect devices with passwords and limit access to those who need it.
Accountability	We can show how we comply: this policy, training records, our record of processing, DPIAs and breach log.

3 Lawful bases

3.1 Before collecting or using personal information, we identify which lawful basis applies. The ones FAM uses most are:

Lawful basis	Typical examples at FAM
Contract	Employment contracts; agreements with sessional workers.
Legal obligation	Payroll and tax records; right to work checks; reporting accidents under RIDDOR 2013; sharing safeguarding information when the law requires it.
Vital interests	Sharing medical information in an emergency when someone cannot consent.
Legitimate interests	Running registers, keeping case notes, managing volunteers, contacting past supporters. We balance our interests against the person's rights and record this in a legitimate interests assessment.
Consent	Photographs and film for publicity, marketing emails, optional newsletters. Consent must be freely given, specific, clear and as easy to withdraw as to give.

3.2 We do not rely on consent where a person cannot really say no, for example where information must be shared to keep someone safe. In those cases we use another lawful basis and explain it honestly.

3.3 The Data (Use and Access) Act 2025 recognises some purposes, such as safeguarding vulnerable people and responding to emergencies, as legitimate interests that do not need a separate balancing test. The Data Protection Lead will confirm when this applies before we rely on it.

4 Special category and criminal offence data

- 4.1** Some information needs extra protection. Special category data includes health (including SEND and mental health), racial or ethnic origin, religious beliefs, sexual orientation, sex life, political opinions, trade union membership, genetic and biometric data. Criminal offence data includes DBS check results and information about offending.
- 4.2** To use this information we need a lawful basis **and** a separate condition under Article 9 of the UK GDPR or Schedule 1 of the Data Protection Act 2018. The conditions FAM usually relies on are explicit consent, employment obligations, vital interests, and the substantial public interest conditions for safeguarding children and individuals at risk and for equality monitoring. Where the Act requires it, we keep an **appropriate policy document** explaining how we protect this information; the Data Protection Lead maintains it.

Immigration status

- 4.3** Many young people in our New to the UK work are refugees or asylum seekers. Immigration status is not a special category under the law, but it is highly sensitive and could cause serious harm if mishandled. We therefore treat it with the same care as special category data:
- We only record immigration status when it is genuinely needed, for example to check eligibility for a funded programme or to make a suitable referral.
 - Where a simple "eligible / not eligible" note will do, we record that instead of the detail.
 - We never copy Home Office documents unless a funder or the law requires it, and we record why.
 - Access is limited to the worker supporting the young person and their manager.
 - We do not share immigration information with any authority unless the law requires it or there is a safeguarding need, and the Data Protection Lead is consulted first.
 - Staff and volunteers must not give immigration advice. See the Referral, Signposting and Immigration Advice Boundaries Policy.

5 Children's data

- 5.1** Children and young people deserve extra protection because they may be less aware of the risks. We:
- Write privacy information in plain language that a young person can understand.
 - Ask for parent or carer consent for under-13s where consent is our lawful basis. For online services offered directly to children, the UK age for a child to give their own consent is 13.
 - For young people aged 13 to 17, consider whether the young person understands what they are agreeing to, and involve parents or carers where appropriate.
 - Follow the ICO's Age Appropriate Design Code when designing any online service young people use.

- Do not profile children or send them marketing unless there is a clear lawful basis and it is in their interests.

5.2 A young person's right to their own information belongs to them, not their parent. Where a parent asks for a child's information, we consider whether the child is mature enough to understand their rights and what is in the child's best interests.

6 Individual rights and how we respond

- 6.1** People have the following rights over their information: to be informed; of access (a subject access request); to rectification; to erasure; to restrict processing; to data portability; to object; and rights relating to automated decision-making. FAM does not make decisions about people by purely automated means.
- (a)** Anyone who receives a request, verbal or written, passes it to the Data Protection Lead the same working day. Requests do not need to use any particular wording.
 - (b)** The Data Protection Lead logs the request and, where needed, checks the person's identity. Where we need more information to find what they want, we ask promptly; the time limit pauses until they reply.
 - (c)** We respond **within one calendar month** of receiving the request. For complex or multiple requests we may extend this by up to two further months, telling the person within the first month and explaining why.
 - (d)** We carry out a reasonable and proportionate search of paper and electronic records, including emails and messaging apps.
 - (e)** We remove information about other people, and consider whether any exemption applies, for example where disclosure could put someone at risk of serious harm. Safeguarding records need particular care; the Designated Safeguarding Lead (DSL) is always consulted.
 - (f)** Responses are free of charge unless the request is clearly unfounded or excessive.
- 6.2** If someone is unhappy with how we have handled their information, they can complain to the Data Protection Lead. We acknowledge data protection complaints within 30 days and deal with them without undue delay, as the Data (Use and Access) Act 2025 requires. People can also complain to the Information Commissioner's Office (ICO).

7 Security

- Paper records are kept in locked cabinets and are not left in cars or on display.
- Devices used for charity work are password or PIN protected and set to lock automatically.
- Personal information is stored on the charity's approved systems and shared drive, not on personal email accounts or unapproved apps.
- Staff and volunteers who use personal phones for work follow the Online Safety, Social Media and Images Policy and delete participant information when no longer needed.
- Records are disposed of securely by shredding or secure deletion.

8 Data breaches

- 8.1** A personal data breach is any security incident that leads to personal information being lost, destroyed, changed, disclosed or accessed without permission. Examples: a lost register, a misdirected email, a stolen phone.
- (a) Report it straight away to the Data Protection Lead, or to the Operations Lead if the Data Protection Lead is not available. Do not wait until you have all the facts.
 - (b) Take immediate steps to contain it, such as asking a wrong recipient to delete an email.
 - (c) The Data Protection Lead assesses the risk to the people affected and records the breach in the breach log, whether or not it is reportable.
 - (d) If the breach is likely to result in a risk to people's rights and freedoms, the Data Protection Lead reports it to the ICO **within 72 hours** of the charity becoming aware of it.
 - (e) If there is a high risk to the people affected, we tell them without undue delay and explain what they can do to protect themselves.
 - (f) The Chair of Trustees is informed. Trustees consider whether it is also a serious incident to report to the Charity Commission, under the Serious Incident Reporting Policy.

9 Data protection by design and DPIAs

- 9.1** We build privacy into new projects, systems and partnerships from the start. Before starting anything new that involves personal information, the project lead talks to the Data Protection Lead.
- 9.2** A **Data Protection Impact Assessment (DPIA)** must be completed before any processing that is likely to result in a high risk to people. At FAM this is likely to include:
- new systems or apps holding information about children or young people;
 - large-scale use of special category or immigration information;
 - new data-sharing arrangements with partners;
 - using location tracking, CCTV or new technology such as AI tools with participant information.
- 9.3** The DPIA describes the processing, assesses necessity and risks, and records the measures taken to reduce them. It is approved by the Data Protection Lead and, for high-risk projects, by the trustees. If a high risk cannot be reduced, we consult the ICO before going ahead.

10 Sharing with partners and suppliers

- 10.1** FAM works with schools, local authorities, employers, youth hubs, football club community trusts and other partners. We only share personal information when there is a lawful basis and it is necessary.

- Regular sharing is covered by a written data sharing agreement setting out what is shared, why, and how it is protected.
- Referrals are made with the young person's knowledge and, where appropriate, agreement.
- Suppliers who handle information for us, such as IT, payroll or cloud providers, are data processors and must have a written contract that meets UK GDPR requirements.
- Safeguarding information is shared under the Safeguarding Children and Young People Policy. Data protection law does not prevent sharing information to keep a child or adult safe.

11 International transfers

- 11.1** Some cloud services store information outside the UK. Before using any such service, the Data Protection Lead checks that the transfer is lawful, for example because the country is covered by UK adequacy regulations, or the supplier uses the UK International Data Transfer Agreement or Addendum. We record which services store data abroad and on what basis.

12 Roles and responsibilities

Role	Responsibilities
Trustees	Overall accountability. Approve this policy, receive breach reports, keep under review whether a Data Protection Officer is required.
Data Protection Lead	Day-to-day lead. Keeps the record of processing, handles rights requests and breaches, advises on DPIAs, arranges training, manages the ICO fee.
Operations Lead	Makes sure systems, contracts and ways of working follow this policy.
Designated Safeguarding Lead	Manages safeguarding records and advises on sharing safeguarding information.
Staff and volunteers	Follow this policy, complete training and report breaches and requests promptly.

Data Protection Officer

- 12.1** FAM is a small charity. The law only requires a Data Protection Officer where an organisation's core activities involve large-scale regular monitoring of people, or large-scale processing of special category or criminal offence data. The trustees consider that FAM does not currently meet this test, so a Data Protection Lead carries out the role instead. **The trustees keep this under review**, particularly as the charity grows or replicates into new towns.

13 ICO fee, training and monitoring

- FAM pays the data protection fee to the ICO unless it confirms, using the ICO's self-assessment, that it is exempt. The Data Protection Lead checks this each year and makes sure the registration is renewed on time.
- All staff and volunteers receive data protection training at induction and refresher training at least every two years.
- The Data Protection Lead reports to trustees at least once a year on requests, breaches, DPIAs and any changes in the law.

14 How this policy supports our focus

- We handle the personal information of young people aged 11 to 25, including special category information about SEND, health, ethnicity and immigration status, which needs extra protection.
- When we use digital and AI tools, no young person's personal information is entered into them unless the tool has been approved for that use.

15 Related policies

- Privacy Notice (Participants, Families and Supporters)
- Safeguarding Children and Young People Policy
- Safeguarding Adults at Risk Policy
- Online Safety, Social Media and Images Policy
- Safer Recruitment and DBS Policy
- Referral, Signposting and Immigration Advice Boundaries Policy
- Serious Incident Reporting Policy
- Complaints Policy
- Code of Conduct and Professional Boundaries (Staff and Volunteers)

Approval record

Approved by the Board of Trustees on	10 th Sep 2026
Signed (Chair of Trustees)	
Next review due	31st July 2027
Version history	1.0, September 2026. New policy; replaces any earlier FAM or FACE version.