Data Protection & GDPR Policy

1. Policy Statement

Ivison Trust is committed to ensuring that all personal data it collects, processes, stores, or shares is handled lawfully, fairly, and transparently in accordance with the UK General Data Protection Regulation (UK GDPR) and the Data Protection Act 2018 (DPA 2018).

We recognise the sensitivity of the personal, special category, and criminal offence data we process, particularly in relation to children, families, and individuals linked to safeguarding concerns, and are committed to protecting the rights and freedoms of all individuals while fulfilling our safeguarding responsibilities.

This policy applies to all staff, trustees, volunteers, sessional workers, contractors, and anyone processing personal data on behalf of Ivison Trust.

2. Legislative and Regulatory Framework

This policy is informed by and complies with the following legislation and guidance:

- UK General Data Protection Regulation (UK GDPR)
- Data Protection Act 2018
- ICO guidance on data protection and information sharing
- Charity Commission guidance on data protection and accountability
- Common law duty of confidentiality
- Relevant safeguarding legislation and statutory guidance

Where Ivison Trust provides or uses online services that may be accessed by children, the Age Appropriate Design Code (Children's Code) is taken into account.

3. Data Protection Principles

Ivison Trust processes personal data in accordance with the principles set out in Article 5 of the UK GDPR:

1. Lawfulness, fairness, and transparency
2. Purpose limitation
3. Data minimisation
4. Accuracy
5. Storage limitation
6. Integrity and confidentiality (security)
7. Accountability

4. Data Protection Officer / Data Protection Lead

Ivison Trust has a Data Protection Officer (DPO) / Data Protection Lead to oversee compliance with data protection legislation.

Responsibilities include:

- Monitoring compliance with UK GDPR and the DPA 2018
- Providing advice on lawful processing, safeguarding, and information sharing
- Maintaining records of processing activities
- Advising on and overseeing Data Protection Impact Assessments (DPIAs)
- Acting as a point of contact for the Information Commissioner's Office (ICO) and data subjects
- Supporting staff training and guidance on data protection

The DPO/Data Protection Lead operates independently and without conflict of interest.

5. Types of Data Processed

5.1 Children and Families

- Personal data (e.g. name, date of birth, contact details)
- Special category data (e.g. health information, safeguarding records, family circumstances, experiences of exploitation or harm)

5.2 Individuals Linked to Safeguarding Concerns

- Personal data
- Criminal offence data and related safeguarding information, including allegations, intelligence, or information received from partner agencies

Criminal offence data is processed in accordance with Article 10 UK GDPR and the relevant provisions of the Data Protection Act 2018.

6. Lawful Bases for Processing

Ivison Trust identifies and documents a lawful basis before processing personal data.

6.1 Article 6 UK GDPR

Depending on the context, processing may be based on one or more of the following:

- Article 6(1)(c) – Legal obligation: where processing is necessary to comply with a legal or statutory duty, including safeguarding and child protection obligations.
- Article 6(1)(d) – Vital interests: where processing is necessary to protect the vital interests of a child or another individual, particularly in safeguarding emergencies.
- Article 6(1)(f) – Legitimate interests: where processing is necessary for Ivison Trust's legitimate interests in delivering services, safeguarding children, and preventing harm, and

where those interests are not overridden by the rights of individuals. Legitimate Interest Assessments (LIAs) are completed where required.
- Article 6(1)(e) – Public task: only where Ivison Trust is carrying out a task in the public interest that is supported by law or formal commissioning arrangements.

6.2 Special Category Data – Article 9 UK GDPR

Special category data is processed only where a valid Article 9 condition applies, including:

- Article 9(2)(g) – reasons of substantial public interest, including safeguarding of children and individuals at risk, and the prevention or detection of unlawful acts, supported by Schedule 1 of the DPA 2018.
- Article 9(2)(c) – vital interests, where an individual is physically or legally incapable of giving consent.

6.3 Criminal Offence Data – Article 10 UK GDPR

Criminal offence data is processed only where:

- A valid Article 6 lawful basis applies; and
- A condition under Schedule 1 of the Data Protection Act 2018 is met, including safeguarding, prevention or detection of crime, or protection of children and individuals at risk.

An Appropriate Policy Document (APD) is maintained in accordance with the DPA 2018.

6.4 Consent

Consent is used only where appropriate and lawful. It is not relied upon for safeguarding or child protection purposes.

- Where consent is required, it will be freely given, specific, informed, and unambiguous.
- Withdrawal of consent does not affect processing carried out on other lawful bases or where safeguarding duties apply.

7. Children's Personal Data and Parental Responsibility

Ivison Trust processes children's personal data only where necessary and lawful.

- Services are generally provided to parents or individuals with parental responsibility rather than directly to children.
- Where consent is relied upon, it is obtained from a person with parental responsibility.
- Where processing is necessary for safeguarding, child protection, vital interests, or to comply with a legal obligation, personal data may be processed without consent.
- Where reliance on parental consent may not be in the best interests of the child, including situations involving suspected abuse or neglect, consent will not be relied upon and appropriate safeguarding action will be taken.

Additional technical and organisational measures are applied to protect children's data.

8. Sharing Personal Data

Personal data is shared only where necessary, proportionate, and lawful.

- Information may be shared with police, children's social care, health services, and other statutory or safeguarding partners where necessary to protect children or individuals at risk, prevent harm, or comply with a legal obligation.
- Information sharing for safeguarding or crime-prevention purposes may take place without consent where a lawful basis applies.
- Where required, data sharing agreements or appropriate contractual safeguards are in place.
- All disclosures are documented to demonstrate accountability.

9. Data Retention and Minimisation

Ivison Trust follows the principles of data minimisation and storage limitation.

- Personal data is retained only for as long as necessary for its lawful purpose.
- Documented retention schedules are in place and reviewed annually.
- Data may be retained beyond standard retention periods where necessary for safeguarding, child protection, or the prevention, detection, or prosecution of criminal offences.
- Extended retention is documented, proportionate, and subject to regular review.
- Data is securely deleted or anonymised when no longer required.

10. Security Measures

Appropriate technical and organisational measures are in place, including:

- Secure, password-protected systems
- Encryption of sensitive data and communications
- Secure storage and disposal of physical records
- Role-based access controls
- Regular staff training on data security and breach reporting

11. Data Subject Rights

Individuals have rights under the UK GDPR, including the right to:

- Access their personal data
- Rectify inaccurate data
- Request erasure (where applicable)
- Restrict or object to processing
- Data portability (where applicable)
- Withdraw consent (where consent is relied upon)
- Lodge a complaint with the ICO

Some rights may be lawfully restricted where necessary to protect others, prevent crime, or comply with safeguarding obligations, in accordance with the Data Protection Act 2018.

12. Personal Data Breaches

Ivison Trust has procedures in place to manage personal data breaches.

- All staff must report suspected or actual breaches immediately.
- Breaches are assessed, contained, and investigated.
- The ICO is notified within 72 hours where required.
- Affected individuals are informed where there is a high risk to their rights and freedoms.
- All breaches are logged and reviewed to support continuous improvement.

13. Accountability, Monitoring, and DPIAs

- Records of processing activities are maintained in accordance with Article 30 UK GDPR.
- Data Protection Impact Assessments are completed for high-risk processing.
- Compliance is monitored through audits and reviews.
- Trustees provide oversight and assurance of compliance.

14. Staff Responsibilities and Training

All staff, trustees, and volunteers must:

- Complete mandatory data protection training on induction and annually
- Follow organisational procedures for data protection and safeguarding
- Report data breaches and concerns promptly

15. Policy Review

This policy is reviewed annually and updated in response to:

- Legislative or regulatory changes
- Organisational changes
- Audit findings, DPIAs, or ICO guidance

Agreed: 26th January 2026
Signed: Gail Gibbons, Chair of Trustees
Review Date: January 2027