IT-001 Data Protection Policy

Approved launch version. Live from 1 September 2026.

Element Society

Data Protection Policy

UK GDPR and Data Protection Act 2018 policy for personal data, safeguarding records, staff records, project records and monitoring.

Status	Approved	Policy number	IT-001
Owner	Christopher Hill, DSL / CEO	Review	Next review by August 2027, and sooner after legal, funder, service, serious incident or material risk change.
Applies to	Staff, trustees, volunteers, sessional workers, contractors and relevant third parties	Approval	Chair of Trustees, on behalf of the Board of Trustees

Replaces | This rebuild replaces the previous GDPR Policy wording and removes outdated legal references. It should be read with the Information Security Policy, Safeguarding Policy, Staff Privacy Notice and Acceptable Use Agreement.

1. Policy statement

Element Society is committed to handling personal data lawfully, fairly, transparently and securely. We process personal data to deliver charitable services, education and Alternative Provision, youth work, safeguarding, employment, governance, finance, fundraising, evaluation and legal compliance.

2. Legal framework

UK General Data Protection Regulation (UK GDPR).

Data Protection Act 2018.

Privacy and Electronic Communications Regulations where electronic marketing or cookies are relevant.

Common law confidentiality where confidential information is involved.

Human Rights Act 1998 where privacy and proportionality are relevant.

Safeguarding guidance and statutory duties relevant to the service being delivered.

3. Scope

This policy applies to all personal data processed by or on behalf of Element Society, including information about children, young people, parents, carers, staff, volunteers, trustees, applicants, contractors, donors, partners, commissioners and other contacts. It applies to paper records, electronic records, cloud systems, devices, email, images, recordings, monitoring logs and safeguarding records.

4. Data protection principles

Lawfulness, fairness and transparency.

Purpose limitation.

Data minimisation.

Accuracy.

Storage limitation.

Integrity and confidentiality.

Accountability.

5. Lawful bases

Element must identify and record an appropriate lawful basis before processing personal data. Common lawful bases include contract, legal obligation, legitimate interests, vital interests, public task where applicable and consent where appropriate. Consent should not be used where another basis is more appropriate or where consent cannot be freely given.

Special category data and criminal offence data require additional conditions. Safeguarding, health, SEND, equality, HR and criminal record information must be handled with restricted access, clear purpose and appropriate retention.

6. Children and young people

Data about children and young people must be handled with particular care. Staff must only collect what is needed, explain use in age-appropriate ways where possible, share on a need-to-know basis, and prioritise safeguarding where there is a conflict between confidentiality and safety.

7. Safeguarding and information sharing

Data protection law does not prevent necessary and proportionate information sharing to keep children safe. Consent should usually be sought for early help and supportive information sharing, but consent is not required where there is a safeguarding or child protection reason to share, where seeking consent would increase risk, or where another lawful basis applies.

8. Monitoring, filtering and DPIAs

Filtering and monitoring of devices, systems and networks may involve personal data. Element will ensure monitoring is lawful, necessary, proportionate and transparent. DPIAs must be completed before high-risk processing, including enhanced staff monitoring, significant safeguarding monitoring systems, new systems processing large volumes of sensitive data, or major changes to device or network monitoring.

9. Individual rights

Right of access.

Right to rectification.

Right to erasure where applicable.

Right to restriction.

Right to data portability where applicable.

Right to object.

Rights relating to automated decision-making where applicable.

Requests must be sent to the Data Protection Lead and responded to within statutory timescales. Identity checks must be proportionate. Requests involving children, safeguarding, third-party data or legal sensitivity must be handled carefully and may require advice.

10. Data breaches

All staff must report suspected personal data breaches immediately. Element will assess risk, contain the breach, record the decision and report to the ICO within 72 hours of awareness where legally required. Affected individuals will be notified where the breach is likely to result in a high risk to their rights and freedoms.

11. Processors and third parties

Third-party processors must be subject to appropriate due diligence, written agreements, security expectations and review. This includes cloud systems, HR systems, email systems, safeguarding systems, filtering and monitoring providers, IT support, payroll, evaluation systems and outsourced services.

12. Retention and disposal

Personal data must not be kept longer than necessary. Retention periods must reflect legal, safeguarding, contractual, insurance, employment, finance and operational requirements. Secure deletion or destruction must be used at the end of retention.

13. Training and accountability

Staff must receive data protection training on induction and regular refreshers. Managers must ensure staff use approved systems, report breaches, keep records secure and follow the Information Security Policy and Staff Acceptable Use Agreement.

Launch evidence and data governance locations

Record / register	Storage route
Staff policy acknowledgements	BreatheHR policy read records
Monitoring/filtering staff acknowledgement records	Google Forms / BreatheHR records as applicable
Data breach log	Google Forms
Subject access request log	Google Workspace
Processor/supplier register	Google Workspace
Retention schedule	Google Workspace
Tell us a worry route	Programme posters using QR code, paper form or named staff route; owned by Deputy DSL; reviewed within 24 hours

Approval and DocuSign signature record

Document status	Approved for launch and ready for DocuSign signature
Approval date	26 August 2026
Live from	1 September 2026
Next scheduled review	August 2027
Approval authority	Chair of Trustees, on behalf of the Board of Trustees
Live document library	Google Workspace
Superseded policy archive	Archive Workspace

Role	Name	Signature	Date
Chair of Trustees	Ian Balshaw	DocuSign signature	26 August 2026
Chief Executive Officer / Policy Owner	Chris Hill	DocuSign signature	26 August 2026

No further document text changes are required after DocuSign signature unless the Board, Chair, CEO or policy owner identifies an error before issue.

Ian

DocuSigned by:
3C7037478C9845A...

27-Aug-26 | 08:31 BST