Data Protection Policy

Formerly GDPR Policy

Approved by:	Lauren Meston	**Date:**	20/08/2026
Last reviewed on:	20/08/2026		
Next review due by:	19/08/2027		

1. Statement of intent

Future Pathways CIC is committed to protecting the personal data of young people, parents/carers, staff, applicants, volunteers, contractors, visitors and partners. We recognise that effective data protection is essential to safeguarding, trust, professional practice and lawful operation of our alternative provision.

This policy replaces the previous GDPR Policy and is renamed Data Protection Policy. It is written to reflect UK GDPR, the Data Protection Act 2018, the Data (Use and Access) Act 2025 and current Department for Education guidance on data protection in schools. It should be read alongside Future Pathways privacy notices, safeguarding, online safety, records management and information-security arrangements.

Safeguarding and data protection
Data protection law does not prevent or limit appropriate information sharing for the purpose of keeping children safe. Staff must share safeguarding concerns with the DSL/DDSL without delay. Where there is a safeguarding risk, fears about data protection must not be allowed to prevent necessary, proportionate and lawful sharing.

2. Purpose and aims

- ensure personal data is processed lawfully, fairly and transparently;
- protect confidential and sensitive information about young people, families, staff and others;
- make clear who is responsible for data protection at Future Pathways;
- support staff to handle personal data securely and confidently;
- ensure safeguarding information is shared lawfully and promptly where required;
- explain rights of individuals and how requests will be handled;
- set out expectations for cyber security, devices, cloud systems, photos/videos, CCTV and AI tools;
- ensure data breaches and complaints are managed promptly and transparently;
- demonstrate accountability through records, training, review and appropriate policies and procedures.

3. Scope

This policy applies to all staff, Directors/Trustees, agency workers, volunteers, trainees, contractors and other adults working for or on behalf of Future Pathways who handle personal data. It applies to information held electronically, on paper, in images/video, in communication systems, on safeguarding platforms, in HR/recruitment files, in finance systems and in any other structured or accessible record.

The policy covers personal data relating to young people, parents/carers, staff, applicants, volunteers, trustees/directors, visitors, contractors, commissioners, partner professionals and any other identifiable person whose information is processed by Future Pathways.

4. Legal and guidance framework

This policy has been developed with regard to:

- UK General Data Protection Regulation (UK GDPR);
- Data Protection Act 2018;
- Data (Use and Access) Act 2025;
- Privacy and Electronic Communications Regulations, where relevant;
- Freedom of Information law where applicable to the legal status of the provision;
- Keeping Children Safe in Education 2026;
- Working Together to Safeguard Children 2026;
- Department for Education guidance: Data protection in schools;
- Information Commissioner's Office guidance, including education, data sharing, children's data, subject access, breaches, direct marketing and AI guidance;
- Education, safeguarding, employment, SEND and retention requirements relevant to the records being processed.

The Data (Use and Access) Act 2025 updates UK data protection law but does not replace UK GDPR or the Data Protection Act 2018. Future Pathways will keep its procedures under review as ICO and DfE guidance develops.

5. Data protection principles

Future Pathways will ensure that personal data is:

- processed lawfully, fairly and transparently;
- collected for specified, explicit and legitimate purposes;
- adequate, relevant and limited to what is necessary;
- accurate and, where necessary, kept up to date;
- kept in identifiable form only for as long as necessary;
- processed securely, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage;
- handled in a way that demonstrates accountability and compliance.

6. Roles and responsibilities

Data Controller

Future Pathways CIC is the Data Controller for personal data it decides to collect and use for its own purposes. In some commissioned or partnership activities, Future Pathways may also act as a processor, joint controller or independent controller depending on the arrangement. This will be clarified in contracts, data-sharing agreements and privacy information where required.

Managing Director

Lauren Meston, Managing Director, has senior organisational responsibility for ensuring appropriate data protection arrangements are in place. This includes ensuring that policies, training, systems, contracts, breach processes and safeguarding information-sharing procedures are implemented and reviewed.

Data Protection Lead

Future Pathways will identify a Data Protection Lead to coordinate day-to-day data protection compliance, respond to requests, maintain relevant records and support staff. If a statutory Data Protection Officer is required because of Future Pathways' legal status or processing activities, an appropriately independent DPO will be appointed and named in privacy notices.

Designated Safeguarding Lead

Lauren Meston is the DSL. The DSL/DDSL team is responsible for ensuring that safeguarding records are kept securely, shared appropriately and transferred safely where required. The DSL will make safeguarding information-sharing decisions where there is risk of harm, while having regard to data protection law and statutory safeguarding guidance.

All staff

- complete data protection and cyber/information-security training appropriate to their role;
- handle personal data only for legitimate work purposes;
- use approved systems and secure storage arrangements;
- keep passwords, devices and records secure;
- check recipients carefully before sending personal data;
- report actual or suspected data breaches immediately;
- share safeguarding concerns with the DSL/DDSL without delay;
- avoid using personal devices, private email or unapproved apps for work records unless expressly authorised and risk assessed;
- challenge or report unsafe data handling practice.

7. Personal data processed by Future Pathways

Future Pathways may process personal data including, but not limited to:

- young person records: identity, contact details, attendance, attainment, behaviour, SEND, EHC plan information, medical information, allergy information, safeguarding records, risk assessments, photographs or video where appropriate;
- parent/carer and family information: contact details, parental responsibility, emergency contacts, communication records, family-support information and safeguarding-related information;
- staff and applicant records: recruitment, safer-recruitment checks, right-to-work, qualifications, references, DBS details, training, performance, payroll, pension, absence, occupational health and disciplinary records;
- commissioner and professional information: referral, placement, review, safeguarding and attendance communications with schools, local authorities, Virtual School, social care, health, police and other agencies;
- visitor and contractor records: sign-in records, identity checks, safeguarding confirmation, CCTV or access-control data where used;
- finance, governance and business records necessary for the running of Future Pathways.

Future Pathways processes special category data and sometimes criminal-offence data where this is necessary for safeguarding, education, SEND, health, employment, safer recruitment or legal compliance. Such data will receive additional protection and access will be limited to those who need it.

8. Lawful bases and special category conditions

Future Pathways will identify a lawful basis for each processing activity. Common lawful bases include legal obligation, public task, contract, vital interests, consent and legitimate interests. Where special category data is processed, an additional Article 9 condition must apply, such as substantial public interest, employment obligations, health/social-care purposes, safeguarding of children and individuals at risk, or explicit consent where appropriate.

Consent will only be used where it is genuinely freely given and the individual has a real choice. In many school/AP contexts, consent is not the correct lawful basis because the processing is necessary for safeguarding, education, legal duties or public functions.

Future Pathways will maintain privacy notices and internal records of processing activities which explain the purposes, lawful basis, categories of data, recipients, retention periods and rights relevant to each main area of processing.

9. Privacy notices and transparency

Future Pathways will provide clear privacy information to young people, parents/carers, staff, applicants and other relevant individuals. Privacy notices should explain what information is collected, why it is used, the lawful basis, who it may be shared with, how long it is kept, individual rights and how to complain.

Information given directly to young people should be age-appropriate and accessible. Where information is collected from another organisation, such as a commissioning school or local authority, Future Pathways will ensure privacy information is available within a reasonable period unless an exemption applies.

10. Information sharing and safeguarding

Future Pathways will share personal data where it is lawful, necessary and proportionate. Safeguarding information may be shared with children's social care, police, health professionals, LADO, commissioning schools, local authorities, Virtual School, CAMHS or other relevant agencies where this is needed to protect a child or support effective safeguarding.

- Staff must not promise secrecy to a young person where information needs to be shared for safeguarding reasons.
- The DSL/DDSL should be consulted where staff are unsure whether information should be shared.
- Where a child is at risk of harm, information should be shared without delay and consent should not be sought if doing so would place the child at increased risk or undermine necessary action.
- The reason for sharing, what was shared, with whom and the decision-maker should be recorded.

- Data minimisation still applies: share what is relevant and necessary, not every record by default.

11. Data security and cyber security

Future Pathways will apply appropriate technical and organisational security measures. These may include role-based access controls, strong passwords and multi-factor authentication where available, encryption, secure cloud services, locked storage, clear-desk practice, audit logs, secure disposal, backup arrangements, antivirus/endpoint protection and staff training.

- Personal data must be stored on approved Future Pathways systems, not unmanaged personal devices or private accounts.
- Email containing sensitive personal data must be checked carefully before sending and protected where appropriate.
- Paper records must be stored securely and not left unattended in classrooms, vehicles or public areas.
- Portable devices and removable media must be encrypted and used only where there is a clear business need.
- Staff must report lost devices, misdirected emails, cyber incidents or unauthorised access immediately.

12. Systems, processors and cloud services

Future Pathways uses digital systems to manage education, safeguarding, attendance, communication, finance, HR and business operations. Before appointing a third-party processor or cloud service, Future Pathways will consider data protection, security, safeguarding, UK/international transfers, retention, access controls, contract terms and breach-reporting arrangements.

Written contracts or data-processing terms will be in place with processors where required. Processors must act only on Future Pathways' documented instructions, keep data secure, support rights requests and notify Future Pathways of breaches promptly.

13. International transfers

Future Pathways will not transfer personal data outside the UK unless an appropriate legal safeguard applies. This may include UK adequacy regulations, the UK International Data Transfer Agreement, UK Addendum to EU Standard Contractual Clauses or another lawful mechanism. Cloud systems and education technology will be checked for transfer arrangements where required.

14. Records of processing, retention and disposal

Future Pathways will keep personal data only for as long as necessary for the purpose for which it was collected, taking account of statutory duties, safeguarding requirements, limitation periods and sector retention guidance. A retention schedule will identify typical retention periods for key record categories.

- Safeguarding records will be retained and transferred in accordance with KCSIE and local safeguarding expectations.
- Recruitment and Single Central Record evidence will be retained in line with safer-recruitment requirements and employment retention periods.
- Medical, SEND, attendance and behaviour records will be retained only for as long as necessary and shared securely on transition where required.
- Paper records will be shredded or securely destroyed when no longer needed.
- Electronic records will be deleted securely or anonymised where continued statistical use is justified.

15. Individual rights

Individuals have rights under data protection law, subject to exemptions and limitations. These may include the right to be informed, access, rectification, erasure, restriction, objection, data portability and rights relating to automated decision-making.

Requests do not have to mention “data protection” or “subject access request”. Staff must forward any request for access to, correction of, deletion of or objection to the use of personal data to the Data Protection Lead/Managing Director immediately.

- Future Pathways will normally respond to rights requests within one calendar month of receipt, subject to lawful extension where the request is complex or numerous.
- Identity may need to be verified before information is released.
- Information about other people may need to be redacted or withheld unless disclosure is lawful and fair.
- Safeguarding, legal privilege, crime prevention, confidential references, exam, employment or management exemptions may apply in limited circumstances.
- Requests from parents/carers for a young person’s information will be considered in light of parental responsibility, the young person’s maturity and best interests, safeguarding and confidentiality.

16. Data breaches and incidents

A personal data breach is a security incident that leads to accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data. Examples include misdirected emails, lost paperwork, lost devices, unauthorised access, ransomware, accidental deletion, inappropriate sharing or failure to redact information.

Immediate reporting
All staff must report an actual or suspected personal data breach immediately to Lauren Meston or the Data Protection Lead. Staff must not delay reporting while trying to investigate or fix the issue alone.

Future Pathways will assess the risk to individuals, take containment action, record the breach and decide whether it must be reported to the Information Commissioner’s Office. Not every breach must be reported to the ICO. Where a breach is likely to result in a risk to individuals’ rights and freedoms, Future Pathways will report it to the ICO without undue delay and, where feasible, within 72 hours of becoming aware of it. Where there is a high risk to individuals, affected people will also be informed without undue delay unless an exception applies.

17. Photos, videos, CCTV and image use

Photographs, video and CCTV images can be personal data and may create additional safeguarding risks, particularly for children and vulnerable young people. Future Pathways will use images only where there is a lawful basis, clear purpose, appropriate transparency and suitable controls.

- Images of young people must not be taken on personal devices unless expressly authorised in exceptional circumstances and transferred/deleted in line with policy.
- Publication of identifiable images will be risk assessed, with particular attention to safeguarding, consent where used, objection, looked-after status, court orders, domestic abuse, exploitation and AI-enabled image misuse.
- CCTV, where used, must have clear signage, defined purposes, controlled access, proportionate retention and a documented process for sharing with police or other agencies.
- Images must not be used in a way that shames, stereotypes or compromises a young person’s dignity or safety.

18. Generative AI, automated tools and profiling

Future Pathways will not enter personal, special category, safeguarding, SEND, medical, HR or confidential information into public generative AI tools unless the tool has been approved, risk assessed and appropriate data protection safeguards are in place. Staff must assume that information entered into unapproved AI tools may not remain private.

Automated decision-making or profiling that produces legal or similarly significant effects will not be used without clear legal basis, transparency, human oversight and appropriate safeguards. AI tools used for administration, assessment, safeguarding support, filtering/monitoring or communications must be assessed for accuracy, bias, security, data retention and children’s rights.

19. Education technology and online platforms

Before procuring or implementing education technology, apps or online platforms that process personal data, Future Pathways will consider necessity, lawful basis, data minimisation, security, child privacy, supplier terms, international transfers, retention, user access and safeguarding impact. The Data Protection Lead, Online Safety Coordinator and DSL should be involved where systems affect young people's data, monitoring, safeguarding or online safety.

20. Data Protection Impact Assessments

A Data Protection Impact Assessment (DPIA) will be completed where processing is likely to result in high risk to individuals, especially children. DPIAs are likely to be needed for new safeguarding or monitoring systems, CCTV changes, AI or automated tools, large-scale processing of special category data, new data-sharing arrangements, new EdTech platforms, biometric systems, or processing that could significantly affect young people.

DPIAs should identify the purpose, lawful basis, necessity, proportionality, risks to individuals and measures to reduce those risks. High-risk processing that cannot be adequately mitigated will not proceed without appropriate advice.

21. Staff training and confidentiality

All staff will receive data protection and information-security training on induction and refresher training at appropriate intervals. Training will cover secure handling, safeguarding information sharing, breach reporting, email security, records, personal devices, AI, photos/video, privacy and individual rights.

Confidentiality obligations continue after employment or engagement ends. Deliberate or reckless misuse of personal data may result in disciplinary action and, where appropriate, referral to external bodies.

22. Complaints and concerns

Concerns about how Future Pathways handles personal data should be raised with Lauren Meston or the Data Protection Lead in the first instance. Future Pathways will handle data protection complaints promptly and use them to improve practice where necessary.

Individuals also have the right to complain to the Information Commissioner's Office. Future Pathways will cooperate with the ICO and follow any binding requirements.

23. Monitoring and review

This policy will be reviewed annually or sooner if legislation, ICO/DfE guidance, processing activity, systems, safeguarding arrangements or organisational structure changes. Future Pathways will monitor compliance through staff training records, breach logs, rights requests, system access reviews, data-sharing agreements, processor checks, safeguarding record reviews and audits where appropriate.

24. Linked policies and documents

- Safeguarding and Child Protection Policy;
- Online Safety and Mobile Phone Policy;
- Safer Recruitment Policy;
- Low-Level Concerns Policy;
- Whistleblowing Policy;
- Complaints Policy;
- SEND Policy;
- Attendance Policy;
- Health and Safety Policy;
- Lone Working Policy;
- Staff Code of Conduct;
- Privacy Notices, Records of Processing, Data Retention Schedule and Data Breach Log.

Appendix 1 - Staff quick guide

Situation	What staff must do
Safeguarding concern	Record and report to DSL/DDSL immediately. Do not delay because of data protection worries.
Misdirected email or lost document	Report immediately to Lauren Meston/Data Protection Lead. Do not try to manage it alone.
Subject access or deletion request	Forward the request immediately. Do not promise an outcome.
Sharing with outside agency	Share only what is necessary and lawful; record what was shared, with whom and why.
Photo/video request	Check purpose, lawful basis, consent/objection and safeguarding risk before use.
AI tool request	Do not enter personal or confidential information into unapproved AI tools.
Uncertain situation	Ask the Data Protection Lead or DSL before acting.

Appendix 2 - Data breach response checklist

- Identify what has happened, when, who is affected and what data is involved.
- Contain the breach: recall email, recover records, disable access, change passwords or isolate affected system where appropriate.
- Inform Lauren Meston/Data Protection Lead immediately.
- Assess risk to individuals, including children, staff and vulnerable people.
- Consider whether safeguarding, police, cyber security, commissioner or local authority notification is required.
- Decide whether the ICO must be notified and record the rationale.
- Decide whether affected individuals must be informed and what support they need.
- Record the breach, actions, timings, decision-making and lessons learned.
- Review controls, training or systems to reduce recurrence.

Appendix 3 - DPIA screening prompts

- Does the activity involve children's data, safeguarding data, SEND data, health data or criminal-offence information?
- Does it involve monitoring, tracking, CCTV, filtering/monitoring, AI, profiling or automated decision support?
- Is a new supplier, cloud system, app or EdTech platform involved?
- Will data be shared with a new organisation or transferred outside the UK?
- Could the processing cause distress, discrimination, exclusion, loss of confidentiality or safeguarding risk if misused?
- Is the data collected limited to what is necessary?
- Have young people and parents/carers been given clear privacy information?
- Are security, access, retention and deletion arrangements clear?
- Has the DSL/Online Safety Coordinator been consulted where young people or safeguarding are affected?

Approval

Signed: L. Meston

Lauren Meston - Managing Director, Future Pathways

Date:20/08/2026

Next review due: 19/08/2027