Policy Name	**DATA PROTECTION**
Relevant To	**Federation ☒** **Bidwell Brook Only ☐** **Ellen Tinkham Only ☐**
Type of Policy	**Model ☒** **School ☐**
Name of Policy Holder	**Christine Walker**
Subject/Department	**GDPR**
Approved By	**Full Governing Body ☐** **CBT Governors ☒** **T&L Governors ☐** **SLT ☐**
Version Date (if applicable)	**4.0 (8th August 2025)**
Date of Last Review	**Autumn Term 2026**
Date of Next Review	**Autumn Term 2027**

Contents

1 Introduction and purpose 3

2 Scope 3

3 Definitions 3

4 Roles and responsibilities 3
- 4.1 Governing Body 3
- 4.2 Executive Head 4
- 4.3 Data Protection Officer 4
- 4.4 Staff, temporary staff, contractors, visitors 4

5 Policy content 4
- 5.1 Data Protection Principles 4
- 5.2 Lawfulness, fairness, and transparency 5
- 5.3 Purpose limitation 7
- 5.4 Data minimisation 7
- 5.5 Accuracy of data 7
- 5.6 Storage limitation and disposal of data 8
- 5.7 Security of personal data 8
- 5.8 Technical security measures 8
- 5.9 Organisational security measures 8
- 5.10 Rights of Data subjects 9
- 5.11 Handling requests 10
- 5.12 Data protection by design and default 10
- 5.13 Joint controller agreements 11
- 5.14 Data processors 11
- 5.15 Record of processing activities 11
- 5.16 Management of personal data breaches 11
- 5.17 Data Protection Impact Assessments 12
- 5.18 Data sharing 13
- 5.19 Appointment of a Data Protection Officer 13

6 Policy history 14

Declaration 17

Appendix 1 18

1 Introduction and purpose

1.1 This policy sets out the Learn to Live Federation's commitment to handling personal data in line with the UK General Data Protection Regulation (UK GDPR), the Data Protection Act 2018, Data (Use and Access) Act 2025 and associated laws governing the processing of personal data in the UK (hereafter known as 'data protection legislation').

1.2 The Federation is the data controller for the personal data it processes and is registered with the Information Commissioner's Office (ICO) under registration number ZC081975 (the Federation's registration number incorporating both Bidwell Brook School and Ellen Tinkham School activities). The registration is reviewed and paid annually to the ICO each January. Details about this registration can be found at www.ico.org.uk

1.3 The purpose of this policy is to explain how the Federation handles personal data under data protection legislation and is to inform staff and other individuals who process personal data on the Federation's behalf of the Federation's expectations.

2 Scope

2.1 This policy applies to the processing of personal data held by the Federation as defined by Article 4 of the UK GDPR, and to the processing of special categories of personal data defined by Article 9 of the UK GDPR.

2.2 This includes personal data held about pupils, parents/carers, staff, temporary staff, governors, visitors and any other identifiable data subjects.

2.3 This policy should be read alongside the Federation ICT Acceptable Use Policy and ICT Code of Conduct Policy, and the Federation Subject Access Request Policy.

3 Definitions

3.1 There are several terms used in data protection legislation and in this policy, which must be understood by those who process personal data held by the Federation. These are:

- Personal data
- Special categories of personal data
- Processing
- Data subject
- Data controller
- Data processor
- Personal data breach

3.2 These terms are explained in Appendix 1.

4 Roles and responsibilities

4.1 **Governing Body**

4.1.1 The Governing Body has overall responsibility for ensuring the Federation implements this policy and continues to demonstrate compliance with data protection legislation.

4.1.2 This policy shall be reviewed by the Governing Body on an annual basis.

4.2 Executive Head

4.2.1 The Executive Head has day-to-day responsibility for ensuring this policy is adopted and adhered to by staff and other individuals processing personal data on the Federation's behalf.

4.3 Data Protection Officer

4.3.1 The Data Protection Officer (DPO) is responsible for carrying out the tasks set out in Article 39 of the UK GDPR. In summary, the DPO is responsible for:

- Informing and advising the Federation of their obligations under the data protection legislation
- Monitoring compliance with data protection policies
- Raising awareness and delivering training to staff
- Carrying out audits on the Federation's processing activities
- Providing advice regarding Data Protection Impact Assessments and ensuring these are reviewed annually
- Co-operating with the Information Commissioner's Office
- Acting as the contact point for data subjects exercising their rights

4.3.2 The Executive Head, following liaison with the DPO where necessary, shall report directly to the Governing Body and Senior Leadership Team and provide regular updates on the Federation's progress and compliance with the data protection legislation.

4.3.3 The Federation's DPO is Jenny Goodall who can be contacted through Nikki Burroughs, Executive Head nikki.burroughs@learntolivefederation.co.uk.

4.4 Staff, temporary staff, contractors, visitors

4.4.1 All staff, temporary staff, contractors, visitors and other individuals processing personal data on behalf of the Federation, are responsible for complying with the contents of this policy.

4.4.2 All individuals shall remain subject to the common law duty of confidentiality when their employment or relationship with the Federation ends. This does not affect an individual's rights in relation to whistleblowing.

4.4.3 Failure to comply with this policy may result in disciplinary action or termination of employment or service contract.

4.4.4 All individuals handling the Federation's data shall be made aware that unauthorised access, use or sharing of data, may constitute a criminal offence under the Data Protection Act 2018 and/or the Computer Misuse Act 1990.

5 Policy content

5.1 Data Protection Principles

5.1.1 The UK GDPR provides a set of principles which govern how the Federation handles personal data. In summary, these principles state that personal data shall be:

- Processed lawfully, fairly and in a transparent manner
- Collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes
- Adequate, relevant, and limited to what is necessary for the purpose it was processed
- Accurate and where necessary kept up to date
- Kept in a form which permits identification of data subjects for no longer than is necessary
- Processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures

5.1.2 The Federation and all individuals processing personal data controlled by the Federation, shall comply with these principles.

5.1.3 The Federation shall have appropriate measures and records in place to demonstrate compliance with each of the principles ('accountability').

5.2 **Lawfulness, fairness, and transparency**

5.2.1 Lawful processing - Personal data will only be processed where there is a lawful basis for doing so. This will be where at least one of the following applies:

- The data subject has given consent
- It is necessary for the performance of a contract or entering into a contract with the data subject
- It is necessary for compliance with a legal obligation
- It is necessary to protect the vital interests of a person
- It is necessary for the performance of a task carried out in the public interest or in the exercise of official duties
- It is necessary for our legitimate interests as a school (where applicable) or third party, except where such interests are overridden by the data subject

5.2.3 When special categories of personal data are processed (for example, health or medical data, racial or ethnic origin, this shall only be done where a lawful basis has been identified from the list above, and one from the following list:

- The data subject has given explicit consent
- The processing is necessary for the purposes of exercising or performing any right or obligation which is imposed on the Federation in relation to employment, social security and social protection law (eg safeguarding individuals at risk; protection against unlawful acts; prevention against fraud)
- It is necessary to protect the vital interests of any person where the data subject is physically or legally incapable of giving consent
- The data has been made public by the data subject
- The processing is necessary for the establishment, exercise, or defence of legal claims
- The processing is necessary in the substantial public interest
- The processing is necessary for health or social care
- The processing is necessary for public health.
- The processing is necessary for archiving, research, or statistical purposes.

5.2.4 Consent - Most of the Federation's processing of personal data will not require consent from data subjects (or their parents/carers as appropriate), as the Federation needs to process this data in order to carry out its official tasks and public duties as an educational setting.

However, there are circumstances when the Federation is required to obtain consent to process personal data, for example:

- To send direct marketing or fundraising information by email or text where the data subject would not have a reasonable expectation that their data would be used in this way or have objected to this
- To take and use photographs, digital or video images and displaying, publishing, or sharing these in a public arena such as:
  - on social media
  - in the school prospectus
  - on the school website
  - in the press/media
  - in the school newsletter
- To share personal data with third parties (for example professionals, agencies, or organisations) where the data subject has a genuine choice as to whether their data will be shared, for example when offering services which the data subject does not have to accept or agree to receive.

When the Federation relies on consent as its lawful basis, it will ensure that the following requirements are met:

- The consent is freely given
- The person giving consent is fully informed and fully understands what they are consenting to and any non-obvious consequences of giving or refusing consent
- There must be a positive indication of consent (opt-in as opposed to opt-out), and consent shall not be assumed as being given if no response has been received
- The person giving their consent will be able to withdraw their consent at any time
- Consent shall be documented so that it may be evidenced and referred to in the future, if necessary

Where consent is being obtained for the collection or use of children's information, consent shall be obtained from a parent or guardian until the child is considered to have sufficient maturity to make the decision themselves (except where this is not in the best interests of the child. In such cases, consent will be obtained from an adult with parental responsibility for that child).

The Federation shall ensure that where consent is obtained, there is a record of this. Where possible, consent shall be obtained in writing. All forms requesting consent shall include a statement informing the person of their right to withdraw, and an email address so they may notify the Federation of any changes or withdrawal of consent.

5.2.5 Fairness and transparency - The Federation shall be fair, open, and transparent in the way it handles personal data, and will publish privacy notices which explain:

- What personal data the school processes and why
- What our lawful basis is when we process that data
- Who we might share that data with
- If we intend to transfer the data abroad
- How long we keep the data for
- What rights data subjects have in relation to their data
- Who our Data Protection Officer is and how to contact them

The privacy notices shall be clear, concise, easily accessible and published on the school's website. All forms collecting personal data shall include reference to the privacy notices and a link provided to their location.

Privacy notices will be provided to parents/carers of pupils when their child is enrolled at the school, which will explain how the Federation handles their own and their child's personal data. This notice will be published on the school's website; parents will be directed to this annually thereafter.

Staff will be given a privacy notice explaining how the Federation handles employee information when they join the Federation and directed to this annually thereafter.

The Federation shall provide privacy notices to other categories of data subjects, as appropriate.

5.3 **Purpose limitation**

5.3.1 The Federation shall collect personal data for specified (for example, as described in the privacy notices), explicit and legitimate purposes and shall not process this data in any way would be considered incompatible with those purposes (for example, using the data for a different and unexpected purpose).

5.4 **Data minimisation**

5.4.1 The Federation shall ensure the personal data it processes is adequate, relevant, and limited to what is necessary for the purpose(s) it was collected for.

5.5 **Accuracy of data**

5.5.1 The Federation shall take all reasonable efforts to ensure the personal data it holds is accurate and where necessary kept up to date. Where personal data is found to be inaccurate, this information will be corrected or erased without delay.

5.5.2 The Federation will send frequent reminders, on at least an annual basis, to parents/carers, pupils and staff to remind them to notify the school of any changes to their contact details or other information.

5.5.3 The Federation shall carry out sample checks of pupil and employee files containing personal data, to ensure the data is accurate and up to date. This will be carried out on an annual basis.

5.6 **Storage limitation and disposal of data**

5.6.1 The Federation shall keep personal data for no longer than is necessary for the purpose(s) of the processing. The Federation shall maintain and follow a Record Retention Schedule which sets out the timeframes for retaining personal data. This schedule shall be published alongside the privacy notices on the websites.

5.6.2 The Federation shall designate responsibility for record disposal/deletion to nominated staff, who shall adhere to the Federation's Record Retention Schedule and ensure the timely and secure disposal of the data.

5.7 **Security of personal data**

5.7.1 The Federation shall have appropriate security in place to protect personal data against unauthorised or accidental access, disclosure, loss, destruction, or damage. This will be achieved by implementing appropriate technical and organisational security measures.

5.8 **Technical security measures**

5.8.1 The Federation shall implement proportionate security measures to protect its network and equipment and the data they contain. This includes, but is not limited to:

- having a Firewall, anti-virus and anti-malware software in place
- applying security patches promptly
- restricting access to systems on a 'need to know' basis
- enforcing strong password policies; passwords shall be a minimum of 8 characters in length; changed at appropriate intervals and not shared or used by others
- the use of 2FA or MFA (2 Factor Authentication / Multi-Factor Authentication) wherever possible, and particularly on accounts which access / contain special category or sensitive personal data
- encrypting laptops, mobile phones, USBs and other portable devices or removable media containing personal data
- regularly backing up data
- regularly testing the Federation's disaster recovery and business continuity plans, to ensure data can be restored in a timely manner in the event of an incident

5.9 **Organisational security measures**

5.9.1 The Federation will ensure the following additional measures are also in place to protect personal data:

- Staff shall sign confidentiality clauses as part of their employment contract
- Data protection awareness training shall be provided to staff during induction and at least every two years thereafter
- Cyber security training, guidance or advice shall be provided to staff on a regular basis

- Policies and guidance shall be in place relating to the handling of personal data whilst during and outside of school. These will be communicated to staff and other individuals as necessary, including policy revisions. A policy declaration shall be signed by staff and retained on their personnel file
- Data protection compliance shall be a regular agenda item in Governing Body and Senior Leadership Team meetings
- Cross cutting shredders and/or confidential waste containers will be available on the school's premises and used to dispose of paperwork containing personal data
- Appropriate equipment and guidance will be available for staff to use and follow when carrying paperwork off school premises
- The Federation's buildings shall be locked when not in use and door entry systems maintained to restrict access to specific areas within the school
- Paper documents and files containing personal data shall be locked in cabinets/cupboards when not in use, and access restricted on a need to know basis
- Procedures shall be in place for visitors coming onto the school's premises. These will include signing in and out at reception, wearing a visitor's badge and being escorted by a school employee
- The Federation shall have procedures in place to identify, report, record, investigate and manage personal data breaches in the event of a security incident

5.10 **Rights of Data subjects**

5.10.1 Data subjects have several rights under data protection legislation. The Federation shall comply with all written requests from data subjects exercising their rights without delay, and within one month at the latest.

5.10.2 Data subjects have the right to:

- Request access to the personal data the Federation holds about them and receive a copy of this information free of charge (the Federation reserves the right to charge for photocopying, postage and packaging)
- Be informed about the use, sharing and storage of their data
- Ask for their data to be deleted when it is no longer needed
- Port (transfer) their data to another organisation in certain circumstances
- Ask for the information the Federation holds about them to be rectified if it is inaccurate or incomplete
- To ask in certain circumstances for the processing of their data to be restricted
- Object to the Federation processing their information for the 'performance of a task carried out in the public interest', except where the Federation can demonstrate compelling legitimate grounds
- Object to the Federation using their information for direct marketing purposes
- Stop the Federation processing their data if the Federation relied on consent as the lawful basis for processing, and they have subsequently withdrawn consent
- complain to the Federation and the Information Commissioner's Office if they are not satisfied with how their personal data has been processed

5.11 **Handling requests**

5.11.1 Data subjects exercising their rights are recommended to put their request in writing and send it to the relevant school (Bidwell Brook School, Shinners Bridge, Dartington TQ9 6JU or Ellen Tinkham School, Hollow Lane, Exeter EX1 3RW or Ellen Tinkham College, Wayside Crescent, Exeter EX1 3LF). Or email Nikki Burroughs, Executive Head nikki.burroughs@learntolivefederation.co.uk. Data subjects can also exercise their rights verbally. In such cases, the Federation will promptly write to the data subject outlining the verbal discussion/request and will ask the data subject to confirm this is accurate.

5.11.2 Data subjects who request a copy of their personal data (known as making a Subject Access Request) may be asked to provide identification to satisfy the Federation of their identity, particularly where the data subject is no longer a pupil, employee or governor at the school. These requests shall be responded to within one month, upon receipt of receiving a valid request and appropriate identification (where requested).

5.11.3 Pupil information requests - Pupils can request access to their own personal data when they have sufficient maturity to understand their rights; know what it means to make such a request and can interpret the information they receive. The Federation will determine this on a case-by-case basis.

Parents or carers may request access to their child's information without the child's consent if the child is not deemed mature enough to understand their rights. However, if the child is considered sufficiently mature, their consent must be obtained before any information is shared.

Where the child attends a maintained or special school, a parent can request a copy of their child's educational record. The parent/carer does not need consent from the child to access this information so long as the disclosure is considered to be in the child's best interests. This type of request is governed the Education (Pupil Information) (England) Regulations 2005. These requests shall be responded to within 15 school days.

When responding to Subject Access Requests (SARs) or pupil information requests, the Federation shall redact the information the data subject or parent/carer is not entitled to receive, in accordance with the exemptions set out in the Data Protection Act 2018.

The Federation shall consult with the Data Protection Officer upon receipt of a Subject Access Request or pupil information request, and again prior to making disclosures in response to these requests.

5.12 **Data protection by design and default**

5.12.1 The Federation shall have appropriate technical and organisational measures in place which are designed to implement the data protection principles in an effective manner, and will ensure that by default, it will only process personal data where it is necessary to do so. The Federation's Data Protection Policy and supplementary policies, procedures and guides, explain how the Federation aims to achieve this.

5.13 **Joint controller agreements**

5.13.1 The Federation shall sign up to agreements with other data controllers where personal data is shared or otherwise processed on a regular basis, where it is necessary to do so.

5.14 **Data processors**

5.14.1 The Federation shall carry out checks with prospective data processors (eg suppliers providing goods or services which involve the processing of personal data on the Federation's behalf) to assess they have appropriate technical and organisational measures that are sufficient to implement the requirements of the data protection legislation and to protect the rights of data subjects.

5.14.2 The appropriateness of data processors will be assessed by the Federation and the Data Protection Officer before the Federation purchases the service. A record will be kept of their findings.

5.14.3 The Federation shall ensure there are appropriate written contracts/Terms of Service in place with data processors, which contain the relevant clauses listed in Article 28 of the UK GDPR.

5.15 **Record of Processing Activities (RoPA)**

5.15.1 The Federation shall maintain a record of its processing activities in line with Article 30 of the UK GDPR. This inventory shall contain the following information:

- Name and contact details of the schools and the Data Protection Officer
- Description of the personal data being processed
- Categories of data subjects
- Purposes of the processing and any recipients of the data
- Information regarding any overseas data transfers and the safeguards around this
- Retention period for holding the data
- General description of the security in place to protect the data

5.15.2 This inventory shall be made available to the Information Commissioner upon request.

5.16 **Management of personal data breaches**

5.16.1 The Federation shall have procedures in place to identify, report, record, investigate and manage personal data breaches (ie security incidents involving personal data). These include security incidents resulting in the:

- Unauthorised or accidental disclosure or access to personal data (breach of confidentiality)
- Unauthorised or accidental alteration of personal data (breach of integrity)
- Accidental or unauthorised loss of access or destruction of personal data (breach of availability)

5.16.2 All security incidents and suspected personal data breaches must be reported to the Data Protection Officer immediately, via the Federation's Executive Head. Security incidents and data breaches should be reported via CPOMs under Data Loss in the first instance. Information can also be emailed to Nikki Burroughs nikki.burroughs@learntolivefederation.co.uk.

5.16.3 All incidents will be recorded in the Federation's data breach log (CPOMs) and investigated by a member of the Senior Leadership Team (or other person as appropriate), under the support and direction of the Federation's Data Protection Officer.

5.16.4 Notification to the ICO and Data Subjects - The Data Protection Officer shall determine whether the Federation must notify the Information Commissioner's Office and data subjects.

Where a breach is likely to result in a risk to the data subject, for example if they could suffer damage, discrimination, disadvantage or distress as a result of the breach, the Data Protection Officer shall notify the Information Commissioner's Office (ICO) within 72 hours of becoming aware of the breach.

If the breach is likely to result in 'high risks' to data subjects, for example if the breach could lead to identity theft, psychological distress, humiliation, reputational damage or physical harm, the Federation shall inform the data subject promptly and without delay.

When informing a data subject of a personal data breach involving their personal data, the Federation shall provide in clear, plain language the:

- Nature of the incident
- Name and contact details of the Data Protection Officer
- Likely consequences of the breach
- Actions taken so far to mitigate possible adverse effects

5.17 **Data Protection Impact Assessments**

5.17.1 The Federation shall carry out Data Protection Impact Assessments (DPIAs) on all processing of personal data, where this is likely to result in high risks to the rights and freedoms of data subjects, particularly when using new technologies. This includes, but is not limited to the following activities:

- Installing and using Closed Circuit Television (CCTV)
- Any sharing of special category data with other organisations
- Using mobile applications to collect or store personal data, particularly about children
- Any storing / processing of special category data
- Use of Artificial Intelligence applications
- Using systems that record large volumes of personal data, particularly where data processors are involved

5.17.2 The results from DPIAs shall be recorded and shared with the Data Protection Officer, who will advise on any privacy risks and mitigations that can be made to reduce the likelihood of these risks materialising. The Data Protection Officer will monitor the outcome of the DPIA, to ensure the mitigations are put in place and that DPIA's are reviewed annually.

5.18 **Data sharing**

5.18.1 The Federation shall adhere to statutory and non-statutory guidance around sharing personal data as set out in the following:

- Keeping Children Safe in Education (DfE 2026)
- Data Sharing Code of Practice (ICO 2020)
- 10 Step Guide to sharing information to safeguard children (ICO)
- DfE Information Sharing Advice for Practitioners providing safeguarding services to children, young people, parents and carers (May 2024)

5.18.2 When sharing personal data with third parties the Federation shall adhere to the following principles:

- Data subject(s) shall be made aware of the sharing through privacy notices or specific communications regarding the sharing
- Identification of an appropriate lawful basis prior to sharing data
- Data shared shall be adequate, relevant and limited to what is necessary
- Accuracy of the data shall be checked prior to the sharing (where possible)
- Expectations regarding data retention shall be communicated
- Data shall be shared by secure means and measures in place to protect the data when received by the third party
- A record shall be kept of the data sharing

5.18.3 The Federation recognises that the data protection laws allow organisations to share necessary personal data with third parties to protect the safety or wellbeing of a child and in urgent or emergency situations to prevent loss of life or serious physical, emotional or mental harm and this is included in the Federation's data protection training for all staff.

5.19 **Appointment of a Data Protection Officer**

5.19.1 The Federation shall appoint a Data Protection Officer to oversee the processing of personal data within the school, in compliance with Articles 37-38 of the GDPR. This person shall be designated based on professional qualities and in particular, expert knowledge of data protection law and practices and the ability to fulfil the tasks referred to in Article 39 of the GDPR.

5.19.2 The Federation shall publish the contact details of the Data Protection Officer and communicate these to the Information Commissioner's Office.

6 Policy history

Policy Version	Summary of Change	Amended by	Implementation Date
V1.0	This policy replaces the Federation's existing Data Protection Policy.	DPO	5 September 2022
V2.0	**Reworded:** 4.3.3 The Federation's DPO is Dave O'Loughlin who can be contacted at Ellen Tinkham School (school@ellentinkham.devon.sch.uk) **Deleted:** 4.3.4 The DPO is supported in their role by a Federation employee, this person is known as the DPO's Data Protection Link Officer. All enquiries, complaints, requests, and suspected breaches of security should be referred to the Data Protection Link Officer in the first instance, who will then notify the DPO. **Reworded:** 5.1.2 The Federation and all individuals processing personal data controlled by the Federation, shall comply with the data protection principles outlined in 5.2 Lawfulness, fairness, and transparency. **Inserted:** 5.1.3 The Federation shall have appropriate measures and records in place to demonstrate compliance with the data protection principles. **Inserted:** **5.18 Data sharing** 5.18.1 The Federation shall adhere to statutory and non-statutory guidance around sharing personal data as set out in the Keeping Children Safe in Education (DfE 2023), Data Sharing Code of Practice (ICO 2020) and Information Sharing Advice for Practitioners providing safeguarding services to children, young people, parents and carers (HM Government 2018). 5.18.2 When sharing personal data with third parties the Federation shall adhere to the following principles: • Data subject(s) shall be made aware of the sharing through privacy notices or specific communications regarding the sharing • Identification of an appropriate lawful basis prior to sharing data • Data shared shall be adequate, relevant and limited to what is necessary • Accuracy of the data shall be checked prior to the sharing (where possible)	DPO	24 July 2023

	• Expectations regarding data retention shall be communicated • Data shall be shared by secure means and measures in place to protect the data when received by the third party • A record shall be kept of the data sharing. 5.18.3 The Federation recognises that the data protection laws allow organisations to share necessary personal data with third parties to protect the safety or wellbeing of a child and in urgent or emergency situations to prevent loss of life or serious physical, emotional or mental harm and this is included in the Federation's data protection training for all staff.		
3.0	This policy replaces the Federation's existing Data Protection Policy. The following paragraph has been amended to reflect the new DfE guidance on Keeping Children Safe in Education for 2024 and to insert a link to this legislation: **5.18 Data sharing** 5.18.1 The Federation shall adhere to statutory and non-statutory guidance around sharing personal data as set out in the Keeping Children Safe in Education (DfE 2024), Data Sharing Code of Practice (ICO 2020) and Information Sharing Advice for Practitioners providing safeguarding services to children, young people, parents and carers (HM Government 2018).	DPO	16 October 2024
4.0	This Policy replaces the Federation's existing Data Protection Policy – changes outlined below:- 1.1 updated to include links to legislation and inclusion of reference to the new Data (Use and Access) Act 2025 2.1 links to Articles 4 and 9 of the UK GDPR added. 3.1 Definition added for 'Personal Data Breach' 4.3.1 – Link added to 'Article 39 of UK GDPR' 4.3.3 – 'Federation email address' changed to 'Federation Data Protection Link Officer email address'. 5.1.1 – change of wording to 5th and 6th bullet points to give additional clarity surrounding the principles. 5.1.2 -and 5.1.3 – change of wording	DPO	8 August 2025

	5.2.7 and 5.2.8 – change of wording to reflect there being no specific age of consent but rather an assessment of a child's maturity to provide consent. 5.2.12 and 5.2.13 – change of wording 5.8.1 – 5th bullet point – reference to Multi-Factor Authentication (MFA) included 5.9.1 – 2nd bullet point – option for bi-annual training added 5.11.5 – New wording implemented regarding children's consent (specific age removed in line with legislation) 5.11.6 – 'special school' added along with wording to reflect considerations for the child's 'best interests'. Link to Education (Pupil Information) (England Regulations 2005 inserted 5.14.3 – link to Article 28 of UK GDPR inserted 5.15.1 – link to Article 30 UK GDPR added 5.17.1 – 'Use of AI applications' added to bullet point list of instances where a DPIA is required 5.18.1 – Links to statutory and non-statutory information sharing guidance added. 5.19.1 – inclusion of links to Articles 37, 38 and 39 of the UK GDPR.		
5	This policy replaces the existing Federation policy, using the model Devon Education Services policy as its basis (v4 August 2025). Minor updates as follows: • Deleted references to the Data Protection Link Officer (name, title, email) and replaced with Executive Head details • 5.18.1 – Changed the Keeping Children Safe in Education link to the 2026 document	Christine Walker	24th August 2026

Declaration

I confirm that I have read, understood and shall adhere to the Learn to Live Federation's Data Protection Policy dated Autumn 2026 to Autumn 2027 and the supporting policies and procedures referred to in this policy.

NAME	
JOB TITLE	
DATE	
SIGNATURE	

Instructions for School Admin

This declaration must be kept in an easily retrieval file. In the case of an employee, this should be kept on their personnel file.

Appendix 1

Data Protection Policy Definitions

Term Used	Summary Definition
Personal data	Personal data means any information relating to an identified or identifiable living individual. This includes a name, identification number, location data, an online identifier, information relating to the physical, physiological, genetic, mental, economic, cultural or social identity of that individual.
Special categories of personal data	Special categories of personal data mean personal data which reveal the racial or ethnic origin, political opinions, religious or philosophical beliefs and the trade union membership of the data subject. It also includes the processing of genetic data, data concerning health, and data relating to an individual's sex life or sexual orientation.
Processing	Processing means any operation or set of operations which is performed on personal data, such as the collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.
Data subject	An identifiable, living individual who is the subject of personal data.
Data controller	A data controller is an organisation who determines the purposes and means of the processing of personal data.
Data processor	A data processor is an organisation who processes personal data on behalf of a data controller, on their instruction.
Personal Data Breach	A personal data breach is a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data.