



DPIA TAPESTRY

May 2025 - 2026

Data Protection Impact Assessment

Submitting controller details

Name of controller	Moorland Federation
Subject/title of DPIA	Tapestry
Name of DPO	SSE Schools DPO dposchools@somerset.gov.uk

Step 1: Identify the need for a DPIA

Explain broadly what the project aims to achieve and what type of processing it involves. You may find it helpful to refer or link to other documents, such as a project proposal. Summarise why you identified the need for a DPIA.

Example:

The school uses Tapestry, an online learning journal, to record children's observations and track Early Years learning. It allows staff to upload photos, videos, and written notes to document educational development, while also allowing parents to access and contribute to their child's profile. Tapestry enhances parent engagement and improves the recording of pupil learning in a secure and consistent way.

A DPIA is necessary because:

- Tapestry involves the processing of pupil data including images and learning assessments.
- Some content may be considered sensitive, particularly where linked to SEND or safeguarding.
- Parents access the data through password-protected accounts.
- Data is stored on cloud servers managed by Amazon Web Services (AWS) within the EU.
- Tapestry acts as the data processor while the school retains the role of data controller.

Step 2: Describe the processing

Describe the nature of the processing: how will you collect, use, store and delete data? What is the source of the data? Will you be sharing data with anyone? You might find it useful to refer to a flow diagram or other way of describing data flows. What types of processing identified as likely high risk are involved?

The Privacy Notice (pupils and parents / workforce) for the school provides the legitimate basis of why the school collects data. Specifically, this relates to keeping children safe on the school site.

How will you collect, use, store and delete data?

Example:

Tapestry collects, stores, and displays observations of children's learning in Early Years settings. Staff upload photos, videos, comments, and assessments. Parents may also upload their own observations and media from home.

What is the source of the data?

Example:

Data is collected from school registration forms, pupil update forms, and staff observations. Parental data is provided via consent forms and includes email addresses. All data is stored on Amazon Web Services (AWS) servers within the EU.

Will you be sharing data with anyone?

Examples:

Data sharing is limited to authorised school staff and parents. Tapestry does not share personal data with third parties without the school's instruction. Tapestry staff with access to data are DBS-checked.

What types of processing identified as likely high risk are involved?

Example:

High-risk processing includes:

- Upload of pupil images and videos
- Communication with parents about SEND or vulnerable pupils
- Potential risks of inappropriate uploads or password misuse

Describe the scope of the processing: what is the nature of the data, and does it include special category or criminal offence data? How much data will you be collecting and using? How often? How long will you keep it? How many individuals are affected? What geographical area does it cover?

What is the nature of the data?

Example:

Each pupil's profile includes:

- Full name and date of birth
- A portfolio of observations linked to EYFS goals
- Attendance and care information (where relevant)

Data also includes information regarding the child's day to day activities within school. Families can also upload information from home to share with school staff.

Special Category data?

Examples:

There will be no special category or criminal offence data collected as defined by the UK GDPR and DPA 2018.

How much data is collected and used and how often?

Example:

Data is collected and used on a regular, ongoing basis throughout the enrolment of the student. Staff upload observations multiple times per week depending on pupil activity. These uploads may include photographs, videos, written notes, and developmental assessments.

How long will you keep the data for?

Example:

Tapestry learning journal data is typically retained for up to 6 months after a pupil leaves the setting. After this period, the school administrator will permanently delete the child's Tapestry account and associated content.

Parents are given the opportunity to download a complete copy of their child's learning journal before deletion. This aligns with good practice on data portability and ensures parents retain a personal copy if desired.

All data retention is managed in accordance with the school's Data Retention Policy.

How many individuals are affected (students, workforce, governors, volunteers)? And what is the geographical area covered?

Example:

The individuals affected are the children and families within the school community.

Describe the context of the processing: what is the nature of your relationship with the individuals? How much control will they have? Would they expect you to use their data in this way? Do they include children or other vulnerable groups? Are there prior concerns over this type of processing or security flaws? Is it novel in any way? What is the current state of technology in this area? Are there any current issues of public concern that you should factor in? Are you signed up to any approved code of conduct or certification scheme (once any have been approved)?

What is the nature of your relationship with the individuals?

Example:

The school collects and processes personal data relating to its pupils/students in order to keep children safe and comply with statutory guidance (KCSIE, Working Together).

Through the Privacy Notices (Pupil/Workforce/Governor/Visitors), the school is committed to being transparent about how it collects and uses data and to meeting its data protection obligations.

Through consent forms, privacy notices, and secure access to Tapestry, the school aims to foster a cooperative, informed, and supportive relationship with families while ensuring compliance with data protection legislation.

How much control will they have?

Example:

Children and families will have limited control over the information recorded on CPOMS. They have the right of access to the records, but redactions may be made if the DSL considers that disclosure may meet the 'serious harm' exemption for educational data in the Data Protection Act 2018. If the data subject or their representative disputes any recorded information, the school will not alter the record but may add a note e.g. *the parent disputes that this incident occurred and has requested that the record is adjusted to reflect their concerns.*

Do they include children or other vulnerable groups?

Example:

The data relates to students including students under 18 years of age (children in law)

Are there prior concerns over this type of processing or security flaws?

Example:

Tapestry is hosted on Amazon Web Services (AWS) infrastructure within the EU, and data is partitioned to ensure each school's data is stored separately. There are no known security flaws.

Describe the purposes of the processing: what do you want to achieve? What is the intended effect on individuals? What are the benefits of the processing – for you, and more broadly?

What do you want to achieve?

Example:

The school aims to provide a secure, effective, and engaging method for documenting children's learning and development in school. The goal is to create a detailed and accessible learning journal for each pupil that captures meaningful observations aligned with the curriculum.

What is the intended effect on individuals?

Example:

For children, it ensures their learning is documented in a rich, meaningful way, supporting early identification of strengths and areas for development. It helps staff plan tailored learning experiences and track developmental progress effectively.

For parents and carers, it improves transparency and strengthens home-school partnerships by providing direct insight into their child's educational journey. Parents feel more connected and engaged with their child's early learning, and are able to contribute their own observations, enhancing the quality of formative assessment.

Tapestry also gives staff a streamlined, secure system for recording and reflecting on pupil progress, reducing administrative burden and enabling more timely, consistent interactions with families.

What are the benefits of the processing – for you, and more broadly?

Example:

For the school:

- Streamlines observation and assessment processes, reducing paperwork
- Enables consistent, high-quality recording of children's learning aligned with EYFS goals
- Provides a secure, centralised platform for storing and managing Early Years data
- Supports safeguarding by ensuring sensitive data is securely stored and accessed only by authorised users
- Saves time for teachers, allowing more focus on teaching and interacting with children

For parents and carers:

- Offers timely and transparent access to their child's learning journey
- Encourages parental engagement and contributions to early education
- Supports continuity between home and school environments

More broadly:

- Enhances early identification of needs and supports inclusive, personalised learning
- Provides a scalable, environmentally friendly alternative to paper records
- Aligns with digital transformation goals in education and supports effective remote engagement when needed (e.g. during school disruption)

Step 3: Consultation process

Consider how to consult with relevant stakeholders: describe when and how you will seek individuals' views – or justify why it's not appropriate to do so. Who else do you need to involve within your organisation? Do you need to ask your processors to assist? Do you plan to consult information security experts, or any other experts?

Example:

- Governors have been consulted.
- The view of the SSE DPO has also been engaged to ensure Data Protection Law compliance

Step 4: Assess necessity and proportionality

Describe compliance and proportionality measures, in particular: what is your lawful basis for processing? Does the processing actually achieve your purpose? Is there another way to achieve the same outcome? How will you prevent function creep? How will you ensure data quality and data minimization? What information will you give individuals? How will you help to support their rights? What measures do you take to ensure processors comply? How do you safeguard any international transfers?

What is your lawful basis for processing?

Example:

The lawful basis for processing personal data is contained in the school's Privacy Notices specifically Article 6(1)(c) Legal Obligation to fulfil our obligations under the following legislation:

- Health and Safety at Work Act
- Keeping Children Safe in Education
- Safeguarding Vulnerable Groups Act
- Working together to Safeguard Children Guidelines (DfE)

Does the processing actually achieve your purpose?

Example:

Tapestry successfully supports the school's aim of improving educational tracking, reducing administrative workload, and fostering a stronger learning partnership between school and home.

Is there another way to achieve the same outcome?

Example:

Possible to record learning using paper-based journals or basic digital alternatives (e.g. shared folders or individual communication apps), these methods lack the structure, security, and functionality of a purpose-built system like Tapestry.

How will you prevent function creep?

Example:

Will be prevented by strictly limiting the use of Tapestry to its intended educational purpose: recording and sharing learning observations. The system is not used for broader data analytics, marketing, or non-educational communication.

How will you ensure data quality and data minimization?

Example:

Measures in place include:

- Clear staff training on the intended use of Tapestry and acceptable data input
- Role-based access control to ensure only relevant staff can view or edit pupil data
- Parental access limited strictly to their own child's profile

- Monitoring of platform use by system administrators to ensure compliance with the agreed scope
- Privacy notices and consent forms that outline specific purposes for data collection and usage

What information will you give individuals?

Example:

The school privacy notice ensures that data subjects and their representatives (e.g. parents) are aware that safeguarding concerns and incidents will be recorded to comply with KCSIE.

How will you help to support their rights?

Example:

The school has a Subject Access Request procedure in place to ensure compliance with Data Protection Law. Other rights e.g. rectification or deletion will be considered where there may be a conflict with the legal responsibilities of the school.

What measures do you take to ensure processors comply? How do you safeguard any international transfers?

Example:

The data on the system is owned by the school and monitored by authorised personnel only. There will be no international transfer.

Step 5: Identify and assess risks

Describe source of risk and nature of potential impact on individuals. Include associated compliance and corporate risks as necessary.	Likelihood of harm Remote, possible or probable	Severity of harm Minimal, significant or severe	Overall risk Low, medium or high
1. Staff password mismanagement (e.g. shared, weak, or lost passwords)	Possible	Significant	Medium
2. Parent password sharing or misuse	Possible	Significant	Medium
3. Inappropriate or excessive content uploaded by staff or parents	Possible	Severe	Medium
4. Retention of pupil data beyond necessary period	Probable	Significant	Medium

Step 6: Identify measures to reduce risk

Identify additional measures you could take to reduce or eliminate risks identified as medium or high risk in step 5				
Risk	Options to reduce or eliminate risk	Effect on risk Eliminated reduced accepted	Residual risk Low, medium, high	Measure approved Yes / No
1. Staff password mismanagement (e.g. shared, weak, or lost passwords)	Example: Enforce strong password requirements (minimum 12 characters), disable autosave, and require password updates each term. Provide regular staff training on secure access practices.	Reduced	Low	Yes
2. Parent password sharing or misuse	Example: Provide parents with secure onboarding instructions and clear guidance on responsible account use. Tapestry enforces password strength and account confirmation on setup.	Reduced	Low	Yes
3. Inappropriate or excessive content uploaded by staff or parents	Example: Ensure staff receive training on appropriate content. Include expectations in the school's Acceptable Use Policy. Monitor uploads and provide clear reporting routes for concerns.	Reduced	Low	Yes
4. Retention of pupil data beyond necessary period	Example: Set a clear retention period (e.g. delete after 6 months of pupil leaving). Ensure administrator reviews and deletes data accordingly. Inform parents in advance and offer journal download.	Reduced	Low	Yes

Step 7: Sign off and record outcomes

Item	Name/position/date	Notes
Measures approved by:	Executive Headteacher	Integrate actions back into project plan, with date and responsibility for completion
Residual risks approved by:	Federation Business Managers	If accepting any residual high risk, consult the ICO before going ahead
DPO advice provided:	Amy Brittan, SSE DPO	DPO should advise on compliance, step 6 measures and whether processing can proceed
<p>Summary of DPO advice:</p> <p>The platform supports the school's commitment to communication and enhances learning engagement while maintaining data protection compliance.</p> <p>Key recommendations include:</p> <ul style="list-style-type: none"> • Ensuring regular staff training on secure and appropriate use • Monitoring password practices and access controls • Reinforcing the 6-month retention policy and parent download option • Ensuring parents are fully informed via updated privacy notices and consent forms <p>Risks identified are mitigated to an acceptable level and that the processing can proceed with the safeguards outlined.</p>		
DPO advice accepted or overruled by:	Executive Headteacher	If overruled, you must explain your reasons
<p>Comments:</p> <p>Advice approved.</p>		
Consultation responses reviewed by:	Federation Business Managers	If your decision departs from individuals' views, you must explain your reasons
<p>Comments:</p>		
This DPIA will kept under review by:	Federation Business Managers	The DPO should also review ongoing compliance with DPIA