HALES VALLEY TRUST

Data Protection Impact Assessment

(Tapestry)

The ICO define Information Society Services as "any service normally provided for remuneration, at a distance, by means of electronic equipment for the processing (including digital compression) and storage of data, and at the individual request of a recipient of a service."

The Data Protection Impact Assessment is a systematic process for identifying and addressing privacy issues and considers the future consequences for privacy of a current or proposed action.

Section 3 Article 35 (1) states "Where a type of processing in particular using new technologies, and taking into account the nature, scope, context and purposes of the processing, is likely to result in a high risk to the rights and freedoms of natural persons, the controller shall, prior to the processing, carry out an assessment of the impact of the envisaged processing operations on the protection of personal data. A single assessment may address a set of similar processing operations that present similar high risks."

Hales Valley Trust use Tapestry. As such **Hales Valley Trust** must consider the privacy implications of the app. The Data Protection Impact Assessment is a systematic process for identifying and addressing privacy issues and considers the future consequences for privacy of a current or proposed action.

Hales Valley Trust recognises that using Tapestry has a number of implications. **Hales Valley Trust** recognises the need to have a good overview of its data information flow.

The Data Protection Impact Assessment looks at the wider context of privacy taking into account Data Protection Law and the Human Rights Act. It considers the need for using an Information Society Services app and the impact it may have on individual privacy.

The school needs to know where the data is stored, how it can be transferred and what access possibilities the school has to its data. If stored in the cloud, the location of the cloud is important to determine applicable law. The school will need to satisfy its responsibilities in determining whether the security measures taken are sufficient, and that the rights of the data subject under the GDPR is satisfied by the school.

Hales Valley Trust recognizes that changes do occur and on this basis good practice recommends that the school review its Data Protection Impact Assessment.

A Data Protection Impact Assessment will typically consist of the following key steps:

1. Identify the need for a DPIA.
2. Describe the information flow.
3. Identify data protection and related risks.
4. Identify data protection solutions to reduce or eliminate the risks.
5. Sign off the outcomes of the DPIA.

Step 1: Identify the need for a DPIA

Explain broadly what 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.
What is the aim of the project? – Tapestry is an online Learning Journal that records children's observation and evidences learning experiences. It can be used to upload photos, videos and written observations. Tapestry enables parents/guardians to have access to their child's profiles and be able to read staff observations and make their own contributions. The information has been used to inform the school's assessment of its children against the Early Years Foundation Stage Framework. The use of Tapestry will also enhance the educational experience, deliver a cost effective solution, and help meet the needs of the business. The school will be complying with Safeguarding Vulnerable Groups Act, and Working together to Safeguard Children Guidelines (DfE). **Hales Valley Trust** will undertake the following processes: 1. Collecting personal data 2. Recording and organizing personal data 3. Structuring and storing personal data 4. Copying personal data 5. Retrieving personal data 6. Deleting personal data By opting for Tapestry the school aims to achieve the following: 1. Scaleability 2. Reliability 3. Management 4. Delivery at a potentially lower cost 5. Supports mobile access to data securely 6. Update of documents in real time (where applicable) 7. Good working practice, i.e. security of access Tapestry is a web based application which uses personal data to set up individual log ins. Tapestry cannot do anything with the school's data unless they have been instructed by the school. The schools Privacy Notice will be updated with reference to Tapestry. The school is the data controller and Tapestry is the data processor.

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 Notices (Pupil) for the school provides the legitimate basis of why **Hales Valley Trust** collects data. The lawful basis in order to process personal data in line with the 'lawfulness, fairness and transparency principle is as follows:

6.1 (c) Processing is necessary for compliance with a legal obligation to which the controller is subject; e.g. health & safety and safeguarding;

6.1 (e) Processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller;

6.1 (f) Processing is necessary for the purposes of the legitimate interest pursued by the controller or by a third party;

The school has highlighted consent as the lawful basis by which it processes personal data. This is recorded in **Hales Valley Trust** Privacy Notice (Pupil).

How will you collect, use, store and delete data? – The information collected by the school is retained on the school's computer systems. Tapestry set-up requires a parent/guardian e-mail address to give access to the app. E-mail accounts are required for each parent/carer. The information is retained according to the school's Data Retention Policy.

What is the source of the data? – Pupil information is collected via registration forms when pupils join the school, pupil update forms the school issue at the start of the year, Common Transfer File (CTF) or secure file transfer from previous schools. Pupil information also includes classroom work, assessments and reports.

Parental/guardian information is obtained by the parent/guardian providing personal data relating to pupil name, their relationship to the child, first and last name of the parent/guardian, and e-mail address. This is provided via a Tapestry consent form issued to the parent/guardian.

Will you be sharing data with anyone? – **Hales Valley Trust** routinely shares pupil information with relevant staff within the school, schools that the pupil attends after leaving, the Local Authority, the Department for Education, Health Services, Learning

Support Services, Management Information Systems and various third party Information Society Services applications including Tapestry.

However concerning Tapestry only staff working at **Hales Valley Trust** can see all of the children's Learning Journeys. No information from Tapestry can be shared with other people without explicit consent of the parents/guardians of those children. Photographs or videos from Tapestry cannot be posted on any social networking site or displayed in a public place (even if they are only about the child of the parent/guardian).

In this instance **Hales Valley Trust** will have obtained explicit consent from the parent/guardian (reference parental consent for use of images for Early Years Foundation Stage) agreeing the child's image being used alongside other children who attend **Hales Valley Trust** respecting learning journeys.

What types of processing identified as likely high risk are involved? – Transferring of personal data from the school to the cloud. Storage of personal data in the Cloud

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? – Pupil data relates to personal identifiers and contacts (such as name, unique pupil number, contact details and address). The Privacy Notice (Pupil) for Tapestry states that the following personal data will be collected: pupil information including the pupil name, date of birth, contents of online Learning Journal including photograph and/or video of the child in different educational settings, records of a child's care, records of a child's attendance. **Hales Valley Trust** as data controller decides exactly what data to include.

Staff are constantly observing and assessing the children in their care. **Hales Valley Trust** takes photographs and videos as evidence of the child's achievements and experiences. The school then use these to assess and monitor each child's progress and identify areas for development.

A Learning Journey is a record of each child's learning and shows snap shots of children's achievements and progress in relation to the Early Years Foundation Stage (EYFS). Not every activity a child does will be recorded, staff will focus on significant moments in each child's learning.

Parental/guardian information will be collected relating to Parent/Guardian name and parent/guardian e-mail address.

Tapestry will be regularly monitored by the Senior Leadership Team.

Special Category data? – Some of the personal data collected falls under the GDPR special category data. When capturing images of the child this will identify the race; ethic origin; and health.

How much data is collected and used and how often? – Personal data is collected for each pupil enrolled in Early Years Foundation Stage. Parents/guardians will only be able to view their own child's information. Parents/guardians will set up an e-mail address, secure password and PIN number to be able to access their child's information only.

Parents/guardians will have access 24 X 7 to their child's Learning Journey.

Parents/guardians can view and contribute to their own child's Learning Journey, receiving a new e-mail whenever a new observation is added to the child's Learning Journey.

Parents can leave a reply/comment on the observations made by staff.

Parents can add their own observations/comments and photos/videos from things their children do at home.

How long will you keep the data for? – When children leave EYFS a copy of their learning journey will be transferred electronically and securely and passed onto the Parents/Carers. The pupils account will be deleted and a sample of the child's learning journey may be stored in line for a limited period for Ofsted and stored securely.

The school will consider the data retention period as outlined in the IRMS Information Management Toolkit for Schools and within the School's Data Retention Policy.

Scope of data obtained? – How many individuals are affected (Pupil). And what is the geographical area covered? Early Years Foundation Stage (EYFS) within the school.

Tapestry will be used to record a child's learning and achievements. It will not be used as a tool for general communication between **Hales Valley Trust** and home and will not be monitored on a daily basis.

However, staff will check regularly for parent replies/comments.

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)?
The school provides education to its students with staff delivering the National Curriculum. **What is the nature of your relationship with the individuals?** – **Hales Valley Trust** collects and processes personal data relating to its pupils and parents to manage the parent/pupil relationship. Through the Privacy Notice (Pupil) **Hales Valley Trust** is committed to being transparent about how it collects and uses data and to meeting its data protection obligation. **How much control will they have?** – On receipt of an e-mail from Tapestry, the parent/guardian is required to confirm their Tapestry account. To ensure that the account is secure the password must be at least 12 characters long, have at least one uppercase letter, one number and one symbol. Tapestry checks the password against a list of common passwords when submitted. Parents/guardians are advised that passwords should be based on random words, be different for each service used, and never be: any family member's name, a pet's name, place of birth, favourite holiday or anything relating to a favourite sports team.

The school will be able to upload personal data from its PC for the data to be stored remotely by a service provider. Any changes made to files are automatically copied across and immediately accessible from other devices the school may have.

Do they include children or other vulnerable groups? – Personal data will relate to Early Years Foundation Stage (EYFS) pupils attending the school. Appropriate password permissions will be insitu to (1) access Tapestry at school; (2) access Tapestry remotely by the parent/guardian and/or; (3) access personal data by the cloud service provider.

Are there prior concerns over this type of processing or security flaws? – Does the third party app provider store the information in an encrypted format? What is the method of file transfer (if applicable)? For example, the most secure way to transfer is to encrypt the data before it leaves the computer.

Hales Valley Trust recognises that moving to a cloud based solution raises a number of General Data Protection Regulations issues as follows:

- **ISSUE:** Tapestry will be storing personal data including special category information. **RISK:** There is a risk of uncontrolled distribution of information to third parties. **MITIGATING ACTION:** Tapestry control access through passwords. Passwords

cannot be seen (technically Tapestry hash passwords before storing them using bcrypt and these are never written to any log files).

Two factor authentication is used to log in. Incorrect password attempts will result in access denied.

Hales Valley Trust uses the option of sending links that allow users to set their own passwords and PIN without the school seeing them.

- **ISSUE:** Lawful basis for processing personal data.
  RISK: GDPR non-compliance.
  MITIGATING ACTION: School has included Tapestry in its Privacy Notice (Pupil) which identifies the lawful basis for processing personal data.

- **ISSUE:** Data Ownership.
  RISK: GDPR non-compliance.
  MITIGATING ACTION: The school as data controller maintains ownership of the data. Tapestry is the data processor. In terms of disclosure Tapestry will not release the information to any third party unless the request is subject to legal obligation without obtaining the express written authority of the school who provided the information.

- **ISSUE:** Data Retention.
  RISK: GDPR non-compliance.
  MITIGATING ACTION: The duration of the processing is, at most, the duration of the contract with the school and the additional time taken for personal data to leave Tapestry's backup system. This can be shorter if the school choose to delete some or all of the data sooner. The application of the data retention period from the school's data retention policy will apply.

- **ISSUE:** Responding to a Data Breach.
  RISK: GDPR non-compliance.
  MITIGATING ACTION: Contract for the Tapestry Online Journal states that if Tapestry becomes aware of, or suspect, a data breach, as data processor they will inform the data controller (the school).

  Tapestry employ independent firms to check its systems are secure by attempting to hack and penetrate them. These firms are accredited by the relevant industry bodies.

The penetration tests include authenticated tests, where testers are provided with login details to Tapestry accounts to check whether they can exploit those to see or extract data that should not be visible.

Tapestry also regularly run automated security tests and carry out internal security reviews.

- **ISSUE:** Third party processor and privacy commitments respecting personal data, i.e. the rights of data subjects.
  RISK: The school is unable to exercise the rights of the individual.
  MITIGATING ACTION: Contract for the Tapestry Online Journal recognises the rights of the data subject concerning the right to be informed, access, rectification, erasure, restrict processing, data portability, object and automated decision making and profiling.

  The data controller is responsible for responding to those requests. Tapestry is designed to assist the data controller respecting such requests.

- **ISSUE:** No deal Brexit.
  RISK: GDPR non-compliance.
  MITIGATING ACTION: In the event of a no deal Brexit Tapestry will probably need to issue a new contract with the set of standard contractual clauses that allow data processing in the UK to remain compliant.

- **ISSUE:** Data is not backed up.
  RISK: GDPR non-compliance.
  MITIGATING ACTION: Tapestry back up data in different locations. At the time of this DPIA the primary physical location is the Republic of Ireland and the backup physical locations are in Germany.

  These backups should be, at most 24 hours old, and Tapestry should have access to 90 days of backups. Backups are primarily for disaster recovery in the event of school data becoming lost or corrupted on the live system.
- **ISSUE:** Subject Access Requests.
  RISK: The school must be able to retrieve the data in a structured format to provide the information to the data subject.
  MITIGATING ACTION: Tapestry have tutorials to assist the school to comply with Subject Access Requests and requests to restrict processing.

  All data on Tapestry will be added by the school (the controller) and is editable. The school also decides when to delete data. By default it will remain in Tapestry backups for 90 days after the school deletes the data however if the school needs data to be removed before then Tapestry is able to assist.

- **ISSUE:** Security of Privacy.
  RISK: GDPR non-compliance.
  MITIGATING ACTION: Tapestry is working towards becoming independently certified as ISO 27001 compliant. Once certification has been achieved the data processor will reissue the contract to the data controller.

  Tapestry's data centre, Amazon Web Services (AWS), has been independently certified as ISO 27001 compliant.

  All Tapestry staff with access to the school's data have been checked and cleared by the Disclosure and Barring Service (DBS) and this is checked annually. AWS also screens its staff.

- **ISSUE**: Transfer of data between the school and the cloud.
  RISK: Risk of compromise and unlawful access when personal data is transferred.
  MITIGATING ACTION: Connection between **Hales Valley Trust** and the Tapestry servers are encrypted. At the moment Tapestry use 2048 bit key, SHA256 with RSA and allow TLS1.0, TLS1.1, and TLS1.2.

  Tapestry uses Enhanced Validation Certification (EVC) providing a visible assurance that the service is being provided by a validated organization. Personal data at rest on Tapestry servers are encrypted.

- **ISSUE:** Cloud Architecture.
  RISK: The school needs to familiarise itself with the underlying technologies the cloud provider uses and the implications these technologies have on security safeguards and protection of the personal data stored in the cloud.
  MITIGATING ACTION: Tapestry network is partitioned to provide minimum access between Tapestry servers and the internet.

  Specifically, Tapestry databases cannot directly access or be accessed from the internet, but only from specific servers. Only a minority of servers can be accessed from the internet, and only specific ports ad using specific protocols. This reduces the risk of external hackers gaining access to Tapestry servers and then getting data out.

  Data held by Tapestry is partitioned so that **Hales Valley Trust** is held in a separate database from that of other accounts. This mitigates the likelihood that a compromise in an account elsewhere would lead to a compromise of the school's data held by Tapestry.

  Tapestry software is partitioned so that it only has the minimum level of privileges to carry out whatever task it is currently doing. This reduces the likelihood that

somebody who hacked into one part of Tapestry's code could use it to compromise other areas.

This should be monitored to address any changes in technology and its impact on data.

- **ISSUE:** Cloud solution and the geographical location of where the data is stored.
  RISK: Within the EU, the physical location of the cloud is a decisive factor to determine which privacy rules apply. However, in other areas other regulations may apply which may not be Data Protection Law compliant.
  MITIGATING ACTION: Data is stored within data centers in the EU. The primary processing and storage location is Ireland.

  Tapestry offsite backups are stored in Germany.

  A data transfer outside of the UK will only happen if Tapestry need to look at the school's data in order to provide additional support.

- **ISSUE:** GDPR Training.
  RISK: GDPR non-compliance.
  MITIGATING ACTION: Appropriate training is undertaken by personnel that have access to Tapestry.

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?
The school moving to a cloud based solution will realise the following benefits: ▪ Scaleability ▪ Reliability ▪ Resilience ▪ Delivery at a potentially lower cost ▪ Supports mobile access to data securely ▪ Update of documents in real time ▪ Good working practice, i.e. secure access to sensitive files

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?
The views of senior leadership team and the Board of Governors will be obtained. Once reviewed the views of stakeholders will be taken into account The view of YourIG 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 minimisation? 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?

The lawful basis for processing personal data is contained in the school's Privacy Notice (Pupil). The Legitimate basis includes the following:

- Childcare Act 2006 (Section 40 (2)(a)
- The Education Reform Act 1988
- Further and Higher Education Act 1992,
- Education Act 1994; 1998; 2002; 2005; 2011
- Health and Safety at Work Act
- Safeguarding Vulnerable Groups Act
- Working together to Safeguard Children Guidelines (DfE)

The school has a Subject Access Request procedure in place to ensure compliance with Data Protection Law

The cloud based solution will enable the school to uphold the rights of the data subject? The right to be informed; the right of access; the right of rectification; the right to erasure; the right to restrict processing; the right to data portability; the right to object; and the right not to be subject to automated decision-making?

The school will continue to be compliant with its Data Protection Policy

Step 5: Identify and assess risks

19

Describe source of risk and nature of potential impact on individuals. Include associated compliance and corporate risks as necessary.	**Likelihood of harm**	**Severity of harm**	**Overall risk**
	Remote, possible or probable	Minimal, significant or severe	Low, medium or high
Data transfer; data could be compromised	Possible	Severe	Medium
Asset protection and resilience	Possible	Significant	Medium
Data Breaches	Possible	Significant	Medium
No deal Brexit	Possible	Significant	Medium
Subject Access Request	Probable	Significant	Medium
Data Retention	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**	**Residual risk**	**Measure approved**
		Eliminated reduced accepted	Low medium high	Yes/no
Data Transfer	Secure network, end to end encryption	Reduced	Medium	Yes
Asset protection & resilience	Data Centre in EU, Certified, Penetration Testing and Audit	Reduced	Medium	Yes
Data Breaches	Documented in contract and owned by school	Reduced	Low	Yes
No deal Brexit	Brexit contingency plans to relocate servers to UK	Reduced	Low	Yes
Subject Access Request	Technical capability to satisfy data subject access request	Reduced	Low	Yes
Data Retention	Implementing school data retention periods in the cloud	Reduced	Low	Yes

Step 7: Sign off and record outcomes

Item	Name/date	Notes
Measures approved by:	**Chief Executive Officer**	Integrate actions back into project plan, with date and responsibility for completion
Residual risks approved by:	**Chief Executive Officer**	If accepting any residual high risk, consult the ICO before going ahead
DPO advice provided:	Yes	DPO should advise on compliance, step 6 measures and whether processing can proceed
Summary of DPO advice: *(1)* Does Tapestry provide the technical capability to ensure the school can comply with rights of access and subject access requests *(i.e. rights to request access, rectification, erasure or to object to processing?)* *(2)* Does the functionality exist to enable the school to respond to subject access requests? *(3)* Does the functionality exist to enable the school to apply appropriate data retention periods? *(i.e. the period for which personal data will be stored)*		
DPO advice accepted or overruled by:	**Yes**	If overruled, you must explain your reasons
Comments: **[DPO Advice provided]**		
Consultation responses reviewed by:	**Central Team** **(Hales Valley Trust)**	If your decision departs from individuals' views, you must explain your reasons
Comments:		

23

This DPIA will kept under review by:	**Central Team (Hales Valley Trust)**	The DPO should also review ongoing compliance with DPIA

24