TAPESTRY

ONLINE LEARNING JOURNAL POLICY

Policy Date: March 2024   Review Date: March 2026

Introduction

Every child in Reception will have a personal 'Online Learning Profile', which will build up a record of their experiences and learning during their time in Reception.

Online learning profiles will record and store observations, comments, photos and videos. This will help staff to record and track children's progress and to identify any needs along with their next learning steps in line with DfE Statutory Framework for Early Years Foundation Stage and Non Statutory Curriculum Guidance.

At St. Paul's we use Tapestry (The Foundation Stage Forum Ltd) to create online learning profiles for children in Reception. Tapestry is a safe and secure system that enables parents/carers to access their child's learning profile at any time via computer and/or an app for mobile devices. Parents/carers may share the profile with their child, family and friends at home and are encouraged to comment on observations, reports or assessments made by the EYFS staff and also to upload photos of their own.

This will help to create a fully holistic view of the child, to build a joint picture of their child's learning and achievement and to strengthen the school's partnership with parents/carers.

For parents/carers without access to the internet, the school will print all information from Tapestry and collate it into the child's folder.

This policy should be read in conjunction with the school's:
- Child Protection and Safeguarding Policy
- Data Protection Policy
- Online Safety Policy
- Photography and Video consent form
- Privacy Notices
- Tapestry's Privacy Policy (https://tapestry.info/privacy-policy.html)

Data Protection, Safety and Confidentiality

The Tapestry Online Learning Journal is compliant with UK data protection legislation (GDPR); our contract with Tapestry is under UK law. Tapestry processes and stores our data within the EU.

All data held on our Tapestry account is owned by St. Paul's C of E (Aided) Primary School; the school is the registered controller of data with the Information Commissioner's Office (ICO) and bound by EYFS Statutory Framework requirements and the GDPR. Tapestry is the data processor.

Data subjects are the people we add to Tapestry; this might be pupils, staff and relatives of pupils. The data we might choose to add includes:

- The names and email addresses of our staff

- The names and dates of birth of pupils in Reception

- The names and email addresses of the parents/carers and relatives of pupils in Reception

- The contents of a learning profile (assessments of children's performance, notes, photographs and videos of the children)

This is not an exhaustive list and we might choose not to add all this data to Tapestry.

We will only put data on Tapestry where we have permission to do so, i.e. if a parent/carer does not give permission for photos of their child to be taken, we will ensure that none of the photos added to Tapestry depict that child. The school is able to correct or delete data they or parents/carers have stored in Tapestry.

For more information on how we process and protect data please refer to our *Data Protection Policy* and *Privacy Notice* that can be found on the school website.

Each Reception class has dedicated, school-owned, password protected tablet devices to take photographs and videos, and to write notes whilst observing the children as part of our duties within the EYFS Statutory Framework.

We ask parents/carers to consent to the use of Tapestry via a Microsoft Form and to the taking, using and storing of digital images of their child in learning profiles/journals and books when the child joins the school. We also ask parents/carers for permission for their child to appear in other children's learning profiles. Consent can be withdrawn/edited at any time by informing the school in writing.

Digital images (photos and videos) will be uploaded to the child's online profile as they are taken. If the digital image cannot be uploaded onto the child's Tapestry Online Journal immediately (i.e. due to limited/no WiFi access), it will be stored on the device until it can be uploaded to the profile. Digital images will at no time be stored on devices for longer than one week.

Tapestry User

As part of our commitment to safeguarding and data protection, only people we trust have access to Tapestry as part of their role. Staff have to sign the *Staff Acceptable Use Agreement (AUA)* and adhere to the school's Child Protection and Safeguarding Policy, Online Safety Policy, Staff Code of Conduct and Data Protection Policy in order to be set up as a Tapestry user.

Users that we set up on Tapestry (staff/relatives) receive links via email that allows them to set their own password and PIN without us seeing them. The school allows users to reset their own password using their email address. Nominated Tapestry managers are also able to reset passwords for staff and relatives. We make accounts immediately inactive if we believe that the password for one or more

accounts has been compromised.

Staff are encouraged to adopt sensible precautions around the use of passwords (e.g. do not share them, do not reuse them, make them hard to guess) All staff Tapestry logins are password and pin protected. Staff are not permitted to download any digital images (photos or videos) onto their own personal devices.

Parents/carers can only access the learning profile of their own child. Parents/carers may input new observations and digital images and add comments to existing observations. They will not be able to edit existing content.

Accessing a Child's Online Learning Profile

Parents/carers have access to their child's online learning profile throughout their time in Reception. When a child comes to the end of their time in Reception, the school will notify parents/carers to download a PDF copy of their child's online learning profile so they have a lasting record of their child's time in Reception.

From the time of this notification, parents/carers have 30 days to download their child's file. After this time period all files/profiles will be deleted in line with GDPR/data protection guidelines.