Tapestry Privacy, Security and Back-up Policy

Table of Contents

Introduction

Security of a software service or product involves many aspects, and satisfying yourself that you should put your trust in a product can and should require that you ask questions of the organisation and people overseeing that security. The following document aims to give you an understanding of who we are and how we have addressed the important issue of protecting the integrity of Tapestry.

The Foundation Stage Forum Ltd

Company information - general

Tapestry was conceived, and is developed and owned by The Foundation Stage Forum Ltd. (The FSF), an early years organisation that has provided resources and support for the early years (EYFS) workforce since February 2003. We have contracts with several dozen local authorities, many of which have been in place for seven years.

The FSF is a VAT registered, limited company, and is registered with the Information Commissioner's Office (ICO) under the following registration number: Z1783069

Our registered office is at:
1, Southdown Avenue
Lewes
East Sussex
BN7 1EL

FSF Directors

The FSF has two directors: Helen and Stephen Edwards.

Stephen Edwards MSc

Steve is the founder of the FSF. He worked for many years as a technical manager for the telecommunications organisation Ericsson, having completed a Masters Degree in information systems in the nineteen-eighties. He became interested in the early years as a result of his wife (Helen, see below) setting up a nursery in their home, and left Ericsson to set up the FSF in 2002 as a resource and support network for the early years workforce. He has been fully occupied with the FSF ever since, conceiving and driving the development of Tapestry as a part of this commitment.

Helen Edwards DPhil

Helen has been working with young children since 1989, firstly as a primary school teacher, and then as a successful nursery owner/manager, followed by employment as a local authority advisor and university tutor, and more recently as an Ofsted inspector. She also holds the EYP status. Her time is now spent between these commitments and advising on EYFS matters both at the FSF and with respect to Tapestry development.

Physical security and data backup measures

The Tapestry web service is hosted on dedicated servers (dedicated in this context means that the physical computers are installed and run exclusively for the use of the FSF) in a high security data centre situated around 20 miles north of London. The servers are managed by a UK company (United Hosting) which vets its personnel to BS7858 standard. The physical security of our servers is implemented using the following measures:

- 3m security fence with rota-spikes and perimeter anti ram-raid barriers.
- Blast proof anti-intruder shielded external windows and doors.
- Proximity access locks on all external and internal doors.
- Interlocked man-trap doors with identity checks before access to data floors is given.
- Each server cabinet has separate locked door access (no open racks).
- Perimeter and internal IP CCTV system monitored 24x7.
- 24x7 on-site security guards with static and mobile patrols.
- All on-site personnel are security vetted to BS7858 standard.
- Only authorised signed in staff are allowed onto the data floor, which is a private closed facility. Identity is established using biometric iris scans.

As well as the application code, all data is held on our servers at the data centre. Backups are taken every day, to a further secure data centre about 10 miles from the main data centre (offsite backup is desirable to protect data in the event of a catastrophic incident in the main data centre). Tapestry has a separate dedicated database server which does not accept external connections. Each Tapestry account has its own database, ensuring that there is no risk of data 'leakage' from one account to another.

Software and configuration security measures

There follows a high level description of some of the security measures we have taken to protect access to data entered into the Tapestry service. For obvious reasons it is not advisable to declare all measures in detail, and a certain amount of obfuscation is in itself a security measure.

Passwords

Passwords are set up on a number of levels for Tapestry users. Setting managers and staff have access to more areas of the system and more data than parents for example. In all cases we use a one way hashing system that takes the plain text password and appends a random

salt. The salt is multiple characters and contains special characters (such as &!%^, etc). We do not store plain text passwords, ever.

SSL (secure connection) certification.

Connections between end-user and the Tapestry servers use SSL certification, the standard device to protect communication over a network. This employs Hypertext Transfer Protocol Secure (HTTPS) to encrypt the data flow between client and server. Its most obvious signature is the padlock icon many internet users are advised to look out for when, for example, using online banking services.

Access to the Tapestry servers

Data Centre and Data Centre staff

The hosting staff, who maintain the integrity of the physical servers and proactively monitor them for software or configuration issues obviously have access. All staff with this level of access have been security vetted to BS7858 standard. This standard screens individuals employed in an environment where the security and safety of people, goods or property is a requirement of the employing organisation's operations or where such security screening is in the public interest.

Additionally, the Data centre is ISO27001 accredited. The ISO 27001 standard is considered to be the fundamental information security standard because it defines the basics of 'building' and controlling an ISMS.

We have engaged a firm of application security testers (also known as White Hat Hackers) who have spent one week investigating the security of Tapestry. They were given parent and staff accounts so that they could test the security from the perspective of authorised users, in addition to potential external threats. We also have regular automated tests which examine the configuration and security of our servers.

FSF staff

The FSF developers also have admin access to the servers. We are a small organisation with developers who have been with us for some years, and they are employed following our normal interview processes. Some time ago we attempted to have all our employees DBS (CRB) checked, and after contacting the DBS service we found there was no facility for vetting via DBS. The DBS response was as follows:

"Access to sensitive data does not enable eligibility with the exception of the following codes.

- *Eligibility code 36 is specifically for those individuals that are working within the Department for Education or the Office for Standards in Education, Children's Services and Skills. If these departments do not cover their area of work then they would not be eligible for a DBS check under category code 36.*
- *There is also Eligibility Code 38. This code relates specifically to staff working within the 'Office of the Public Guardian' with access to data relating to children and vulnerable adults.*

Unless the staff in question, therefore, qualify under category codes 36 or 38 then there is no eligibility for staff whose sole access to children or vulnerable adults is via documentation or database details."

There is evidently no facility for the FSF to obtain DBS checks on staff, who are not eligible. Nevertheless, the FSF does follow a robust recruitment, induction and supervision process, and we believe we have a secure team who follow strict safeguarding policies. Although it has not proven possible to provide an exhaustive current check, in practical terms most engaged staff have either current, or previous CRB/DBS checks as a result of their wider responsibilities and experience in the early years sector.

Privacy and data ownership

Who owns my data?

In short, you, the Tapestry account manager, own the data. We will not access your Tapestry accounts without your permission. No element of the Tapestry information you input into your accounts, including the email addresses of your staff and parents, belongs to us. We will never attempt to contact your parents directly, for marketing or other purposes. Nor will we pass on your details to any other party.

Who will access my accounts?

Only you, and those you authorise, will visit your Tapestry accounts. If we need to access your account to sort out a problem you are having, we will ask your permission first, and you will need to set up an account for us to do so, which of course you can disable afterwards. We will not give Tapestry account information, or access to your Tapestry account, to anyone other than those individuals you have set up as staff members. Parents contacting us for access details will always be referred to you, the Tapestry account holder.

Can I have my data and accounts deleted?

Yes. If you decide to discontinue Tapestry, we will completely delete all data and media associated with it. As children leave your setting, you can move them into a 'deleted' area,

where (after a delay of thirty days to avoid disastrous mistakes occurring) their records, data and media will be irreversibly deleted.

Is there a limit to the amount of data I can upload?

Currently there is no limit to the amount of text, photos and videos you can upload for a child. However, if we deem there to have been excessive amounts uploaded, we may need to discuss with you the possibility of an increase in subscription fee for the increased storage capacity required. So far, this has not been required for any of our Tapestry subscribers.

What happens if my account subscription should expire?

Obviously we want to avoid painful mistakes happening. For example, some subscriptions inevitably come up for renewal during a school holiday, and it would be unfortunate to say the least, if a manager's non-availability to renew were to result in the deletion of their entire database. We, therefore, do not have an automated deletion process, and will always make attempts to contact the main contact for an expired Tapestry account before final deletion.

After a significant period of time, however, if we are completely unable to make contact with the main contact, and the account has been rendered inactive due to an expired subscription, we will make the decision to delete the account.

What are my responsibilities?

As the data controller, the Tapestry account holder has overall responsibility for complying with the Data Protection Agency requirements.

When taking out a Tapestry subscription, you agree to our Tapestry Terms and Conditions which set out our responsibilities and yours. The Tapestry Terms and Conditions are available from the Foundation Stage Forum website (http://eyfs.info)

Actions for you to consider are:

- Training staff in the use of Tapestry, explaining sensible precautions such as keeping all access details confidential, and not permitting any material to be used without written permission from the parents/carers.
- Delete staff from your Tapestry account once they have left your employment.
- Prevent access to Tapestry from staff who are involved in disciplinary procedures.
- Prevent access to Tapestry for parents whose children have been made inactive or have been deleted, unless they have other children at your setting.
- Giving parents instructions for keeping the data protected, eg by insisting no photos are uploaded to social media sites without the written permission of the parents whose children are depicted in photos, videos or text.

Additional Information

Does the app store data on the tablet? If so, how is it protected?

The default is for the data NOT to be stored on devices, but this can be changed on a setting by setting basis, so that images and video can be left on the device. This is changed by the Tapestry account holder or manager in the admin/management area. If managers decide to retain media on their tablet, then they are not protected and suitable policies must be drawn up by the setting.

How is a particular instance of the tablet application authenticated for use against a particular instance of your solution? Is there any device level enrolment or verification of a tablet device?

No device level enrolment occurs. The application is freely downloadable from the relevant store. Authentication and access is controlled by a login to the server (email address and password). Password complexity can be controlled by the managers of the individual setting (eg specification of digits, upper/lower case, minimum length, etc).

How are user passwords generated in your solution?

Managers of a Tapestry account can generate passwords for their staff and managers manually if required. It is also possible (and recommended) that managers select the option to automatically generate a password via an email that requires account activation. Either way, once this has been done users can re-set their own passwords, but the setting manager controls how complex the passwords are (see answer above). We will be working to add the option of multi-factor authentication in the near future.

Are passwords encrypted?

Yes, passwords are encrypted (we use bcrypt).

How many password attempts before lock out?

Three incorrect password attempts cause a lock out.

How does Tapestry prevent a user being able to search or see information which they are not authorised to see?

The system is designed from the ground up to give permission based access. Therefore, parents, PIN only staff, full staff and managers all have different levels of access. Once they have logged in, content is presented based on this access level. Additionally, each setting has its own dedicated database, preventing cross contamination. These are in a locked down DB server that does not accept incoming connections (ie can only be accessed through our other servers).

Is data at rest encrypted?

No, data at rest is not encrypted (with the exception of passwords). We take the view that if an unauthorised person has gained access to our own dedicated servers, they will also have access to the cipher keys rendering encryption at rest useless. We review this from time to time, but the extra costs in time and server resources of decrypting on the fly so far outweigh the benefits of encryption at rest.

What encryption principles are used for data in transit?

HTTPS- asymmetric. 2048 bit key, SHA256.

What Tapestry account information do the FSF and Tapestry staff have access to?

Although we can access the raw database and media we do not have access to Tapestry accounts without the permission of the Tapestry account holder/manager, who will need to set us up with a temporary login for troubleshooting purposes. They, therefore, control our access to children's learning journals. After troubleshooting, we request that the manager deletes us from their account so they can be assured that we no longer have access.

What Crypto key management processes are in place?

Access to our keys is restricted to our datacentre engineers (all vetted to BS7858), our own Foundation Stage Forum Ltd) developers and technical staff (vetted according to our own employment criteris) and our SSL provider (Globalsign).

The Data centre hosting Tapestry is IS027001 accredited. Which version of IS027001 is it, and who is the accrediting company?

The version is 2013, and the accrediting company is BMTRADA.

What version of SSL do you use?

Our SSL protocols allow TLS1.0, TLS1.1, and TLS1.2. TLS1.3 is currently in working draft and we'll implement it when ready.

What database is used and what version?

Percona 5.6

Has Tapestry ever been independently verified, by a penetration test? If so, can you share the results?

Yes, a penetration test was carried out soon after we launched Tapestry. Our report is confidential and for our developers' use only. However, any recommendations were carefully considered and where necessary any remedial action was taken.

We are currently rebuilding the core Tapestry framework, which will be ready for implementation in the spring of 2016. As this nears completion, we will be running a repeat of the external commissioned penetration test. At our weekly developers meeting, security is always an agenda item, and we decided recently to use owasp.org resources to develop our own internal regular application penetration tests for Tapestry v2.