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.

Security Responsibilities

Security is only as strong as the weakest link. We therefore need to work with you, the account holder, together with any staff and relatives you give permission to use Tapestry to ensure the overall system is secure. This document explains what we do and what we hope you will do.

The latest copy of this document, together with our terms and conditions are always available in the control panel of your copy of Tapestry.

Who are we?

Tapestry is the name of a product that was conceived, developed and is 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 ten or more years.

The Foundation Stage Forum Ltd

The Foundation Stage Forum Ltd is a VAT registered, private UK limited company.

Our company number is 05757213.

Our registered office is at:

```
1, Southdown Avenue
Lewes
East Sussex
BN7 1EL
```

You can write to us at our registered office, or email us at *customer.service@eyfs.info*.

Our contracts are under UK law.

The Foundation Stage Forum 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.

Steve is the board member responsible for security.

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.

Who owns the data?

In short, you, the Tapestry account manager, own the data you put on Tapestry. We, Foundation Stage Forum Ltd, do not. In technical terms, you are the Data Controller, we are the Data Processor.

We will only do things with data that you, or people that you give permission to, request.

We will not access your Tapestry accounts without your permission.

We only use the data you enter to provide the service you see: an online learning journal that helps childminders, schools and nurseries to monitor the progress of their children, communicate with parents and the government and manage their activities.

To be absolutely clear: we don't use the data for marketing; we don't share the data with others to do marketing.

You should be aware of your responsibilities as a data controller. You can find out more at the Information Commissioner's Office website: *https://ico.org.uk/for-organisations/*

You are responsible for making sure that you only put data on Tapestry where you have permission to do so. i.e., if a parent has agreed with you that no photos of their child should be taken, you are responsible for ensuring that none of the photos added to Tapestry depict that child.

Registration with the ICO

The Foundation Stage Forum Ltd is registered with the Information Commissioner's Office (ICO) under the following registration number: Z1783069.

As a data controller, you may also need to be registered with the Information Commissioner's Office. The ICO has guidance on how to work out whether you need to register at *https://ico.org.uk*.

ICO data protection principles

We conform to the eight data protection principles of Schedule 1 of the Data Protection Act:

> Personal data shall be processed fairly and lawfully and, in particular, shall not be processed unless –
>
> (a) at least one of the conditions in Schedule 2 is met, and
>
> (b) in the case of sensitive personal data, at least one of the conditions in Schedule 3 is also met.
>
> Personal data shall be obtained only for one or more specified and lawful purposes, and shall not be further processed in any manner incompatible with that purpose or those purposes.
>
> Personal data shall be adequate, relevant and not excessive in relation to the purpose or purposes for which they are processed.
>
> Personal data shall be accurate and, where necessary, kept up to date.
>
> Personal data processed for any purpose or purposes shall not be kept for longer than is necessary for that purpose or those purposes.
>
> Personal data shall be processed in accordance with the rights of data subjects under this Act.

> Appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data.
>
> Personal data shall not be transferred to a country or territory outside the European Economic Area unless that country or territory ensures an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data

However, this is a partnership between you, as the data controller, and us as the data processor. So you should also make sure that you conform to the principles in the data you enter.

In particular:

- Although most of the data you collect and then place in Tapestry is likely to be necessary for you to run your nursery, childminding service or school you may want to think about whether some of the data is sensitive enough that you should ask for explicit permission.
- You need to ensure that the data you enter is accurate and up to date.
- You need to tell us to delete data that is no longer needed by you (by, for instance, marking a child as having left your setting).

GDPR Compliance

Data protection law is changing and the new laws, known as GDPR will be enforced from May 25 2018.

In preparation for this:

- We have appointed a Data Protection Officer: Lauren Foley dpo@eyfs.info
- We will be updating our contracts with you. This will not change our service or fundamentally change our relationship with you but it will state clearly and unambiguously how we work together to comply with the GDPR. Drafts of the new contract will be available by Christmas 2017 for feedback.

Access to data

Only you, and those you authorise, will have access to your Tapestry accounts. You can restrict the people you authorise to only be able to view data about some children.

If we need to access your account to sort out a problem you are having, we will ask your permission first.

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.

Relatives contacting us for access details will always be referred to you, the Tapestry account holder.

Under the data protection act, individuals have a right to see a copy of information that an organisation holds about them. As the data controller, you will need to respond to those requests and we, as the data processor, will help you. This is normally easy, since you can always see and print the information you have entered.

Deleting data when it is no longer needed

You can modify and delete the data you enter.

In the common case of children leaving your setting, you can move them into a 'deleted' area, where (after a delay of ninety days to avoid disastrous mistakes occurring) their data will be deleted (this includes relevant pictures, videos, journals and reports).

You can instruct us to delete *all* your data at any time. But this is all or nothing. If you just want to delete *some* of your data, you will need to use the control panel in the system to do so yourself.

If you let your subscription to Tapestry lapse, we will delete all data associated with it. We normally delay the deletion in case your subscription has inadvertently lapsed (e.g., it happened while you are on holiday, or there was a delay in your Local Authority paying our invoice) but if you explicitly ask us to then we will delete your data immediately.

In some cases, some data may remain in our backups until those backups are rotated. If you wish, you can instruct us to to delete *all* your data from these backups. But it is all or nothing. We cannot delete *some* of your data on these backups.

Organisational data security

Staff

We are careful in who we employ. All our staff with access to your data have been checked and cleared by the Disclosure and Barring Service (DBS) and we check their DBS status annually.

The company that hosts our servers and databases, AWS, also vets their staff (though in practice we would never expect them to see your data).

You are responsible for only giving access to Tapestry to people you trust and who actually need access. For instance, please remember to make staff inactive once they have left your service or if they are facing relevant disciplinary procedures.

Please also ensure that, when you give access to relatives of children, you are careful to allocate them to the correct children, to enter their email address correctly, and to make them inactive once the child has left your setting.

Procedures

Our procedures are designed to minimise our access to your data. For example, we wouldn't log into your account without your permission and even then would only do so if it was necessary to resolve a fault or problem you were experiencing.

We are similarly careful with our suppliers. The company that hosts our servers and databases, AWS, operates on a similar principle of minimal access. They are ISO27001 accredited, which means they have a complete and appropriate set of security procedures. We would never expect them to need to access to your data.

It is important that you think about your procedures for what sort of data you put on and what you allow your staff and relatives to do with it.

For instance, you should think about:

- Whether you give all staff access to data about all children, or just some children.
- When it is appropriate for your staff to take and share photos and videos.
- What instructions you should give to parents as to what is appropriate for them to add, and what they may do with material that you add (e.g., insisting no photos are uploaded to social media sites by parents without the written permission of the parents whose children are depicted in photos, videos or text.)

Passwords

The main way we control access to Tapestry is through passwords.

Neither you, nor we, can see what passwords have been used (technically, we hash the passwords before storing them using bcrypt and we never write passwords to any log files).

Our staff use strong passwords and, for many of the more secure systems, have to supplement the correct password with other security measures (such as logging in from our office IP address and/or using two-factor authentication).

You are responsible for training your staff, and encouraging any relatives, to adopt sensible precautions around their use of passwords – don't share them, don't reuse them, and make them hard to guess.

Incorrect password attempts will result in an access for that user being prevented for a period of time. If you suspect one of your staff or relative accounts has or could have been compromised, you can make it inactive. This will prevent access using that account. At a minimum, you should then contact the staff or relative and ask them to change their password on this system and any other system on which they have used a similar password.

You can choose a minimum password strength that you permit the people you add to Tapestry to use. We won't let this minimum be any less than 6 characters and we allow and encourage you to set a tougher standard than that (by, for instance, requiring longer passwords or passwords that have symbols, numbers, upper case letters etc.).

For your staff, we also provide an option where they cannot login without a different member of staff (such as a manager) logging in first. We call this PIN only staff.

If you wish, you can set an initial password and PIN for the staff and relatives that you add. But we strongly suggest that if you do, you encourage staff and relatives to then change the password to something only they know.

We allow users to reset their own passwords using their email address. You, and managers you nominate, can also reset passwords for staff and relatives. If a member of staff or relative contacts us because they have lost access to the email address associated with an account, we will direct them back to you.

If you have lost access to your email address associated with Tapestry, or you have taken over a Tapestry account due to the departure of the previous account owner and don't have access, then we can manually change the password and email address of the account owner. However, before doing so, we will take steps to independently verify your identity which means the process will be slow.

We do not currently have a facility for you to restrict access to particular locations or particular devices. That makes it doubly important that you take sensible precautions over passwords.

Technical data security

The Tapestry web service and data are hosted in a cloud hosting environment operated by AWS in the EU (primarily the Republic of Ireland, with backups in Germany). AWS is the largest cloud hosting provider in the world and provides a secure platform for some of the world's largest online service providers.

Physical security

AWS ensure that our servers are physically secure. AWS data centres are housed in nondescript facilities. Physical access is strictly controlled both at the perimeter and at building ingress points by professional security staff utilizing video surveillance, intrusion detection systems, and other electronic means. Authorized staff must pass two-factor authentication a minimum of two times to access data centre floors. All visitors and contractors are required to present identification and are signed in and continually escorted by authorized staff.

AWS only provides data centre access and information to employees and contractors who have a legitimate business need for such privileges. When an employee no longer has a business need for these privileges, his or her access is immediately revoked, even if they continue to be an employee of AWS. All physical access to data centres by AWS employees is logged and audited routinely.

We make sure that the devices we use to connect to the Tapestry servers are physically secure. We also don't store any of your data on our local devices – it is only on the servers.

It is important that you make sure that the devices you use to connect with Tapestry are physically secure. In particular, if you use some form of password manager on a device that remembers you Tapestry password then, at a minimum, make sure that the device also requires a password to login or unlock.

The Tapestry website doesn't store data that you have entered on your laptop or desktop. Therefore, if your computer is stolen, so long as the password wasn't stored on the computer then the person who stole the computer will not be able to access Tapestry data without guessing your password.

If you were logged into Tapestry when your laptop or desktop was stolen then, so long as the browser is open and the machine hasn't been switched off, the person who stole the computer has a short time when they could use your account. Therefore it is important that you either log off when you leave a computer unattended, or ensure your computer automatically locks its screen when you leave it and requires a secure password to unlock.

The iOS and Android Tapestry apps don't store passwords locally, only temporarily store some data (such as copies of images that are being shown on screen), and require a password or pin to be entered to open the app. Therefore, if the device is stolen, the person who stole it would not have significant access to Tapestry data without guessing your password or PIN.

The apps may have local copies of the pictures and videos that have been taken on that device, though there is a setting to prevent those local copies if the pictures and videos were taken from within the app. Similarly, if you download data (such as PDFS of journals) from Tapestry to your device, those are at risk.

Software security

We, together with AWS ensure that the software running on our servers is up to date. We run regular automated tests and internal security reviews to examine the configuration and security of our servers.

Similarly, we ensure that the devices we use to connect to Tapestry are up to date and free from viruses and compromising software.

It is important that you take similar care with the devices you use to connect to Tapestry to ensure they are up to date and free from viruses or compromising software. If you give relatives access, please also encourage them to do the same.

Encryption

Connections between you and the Tapestry servers are encrypted. Tapestry uses Enhanced Validation Certification (EVC), which does not offer any greater degree of technical protection (encryption is still performed at the same strength) but does offer a visible assurance that the service is being provided by a validated organisation (the Foundation Stage Forum Ltd).

Connections between the iOS and Tapestry apps are similarly encrypted.

Connections between our office computers and Tapestry are encrypted.

Your data in AWS is encrypted at rest on our servers. This includes our backups of your data.

It is important that you check, and encourage those who you give access to check, that they are connected to the official Tapestry site before entering their password. The correct URL is *https://tapestryjournal.com*. There should be a padlock or similar symbol to show that the connection is encrypted. Clicking on the padlock or symbol should provide you with information about the connection which should include the fact that the site is owned by the Foundation Stage Forum Ltd.

The SHA1 fingerprint of our certificate is DC F6 23 A3 35 97 98 98 6E 6B 29 91 51 B2 35 93 DA 1F 7F DC

Partitioning

Our network is partitioned to provide minimum access between our servers and the internet. In particular, our databases cannot directly access or be accessed from the internet, but only from specific servers. Only a handful of servers can be accessed from the internet, and only on specific ports and using specific protocols (e.g., no unencrypted connections are permitted). This reduces the

likelihood that external hackers can gain access to our servers and then get data out.

Our data is partitioned so that your data is held in a separate database from that of other accounts. This reduces the likelihood that a compromise in somebody elses's account (because, for instance, they use an easily guessable password) would lead to a compromise of your data.

Our 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 our code could use it to compromise other areas.

Logging

We log activity on our system. Some of these logs are available to you in the Tapestry control panel. We retain more detailed logs to help diagnose and fix faults.

Verification (also known as Penetration Testing)

We employ independent firms to check that our systems are secure by attempting to hack or penetrate them. These firms are accredited by the relevant industry bodies.

The most recent was check was in July 2016. If you have a legitimate interest in Tapestry (e.g., you are the account owner or a parent) we are happy to provide you with their summary of what they found.

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

Capacity, Redundancy and Backups

Our system's capacity scales to meet demand. We do not currently limit the number of users, or the amount of data that they store, we just add the required storage and servers to meet the demand, in most cases automatically.

If a particular account is using our system excessively we may need to discuss the possibility of an increased subscription fee, but we have never yet had to do this.

Our system is redundant and should survive the loss of any server or, indeed, the loss of a physical data centre. This means that we have at least two copies of each operational server and all data is stored in at least two locations.

We also retain backups of all data in a different physical location (at the time of writing, the primarily physical locations are in the Republic of Ireland, the backup physical locations are in Germany). These backups should be, at most, 12 hours old and we should have at least 30 days of backups. The backups are treated with the same care as the primary data (in particular, they are encrypted in transit and rest and stored in AWS facilities with the same physical security as described in the 'physical security' section above).

Keeping in touch about security

If you suspect a security issue (e.g., you believe that passwords on your account may be compromised because, for instance, computers have been stolen) then email us at *customer.service@eyfs.info*. Please include a descriptive subject line in your email (i.e., don't just say "Help!" but say "Help! Our computers have been stolen").

If we have a security concern about your account, we will try and email the primary contact we have listed. This will initially be the person that set up the account. You can change this using the Control Panel within Tapestry (Settings > Contact Details). Please keep this information up to date.

If you or we suspect a security problem, our first step will usually be to lock down the accounts whilst we work together to establish what happened and the best course of action.

Frequently asked questions

Below are some frequently asked questions that relate to security. If you have a question that hasn't been covered by this document, please ask us at *customer.service@eyfs.info*. Please note that, for security reasons, we may not answer some questions (such as, for instance, the exact versions of software that we are using).

Can you fill out this security questionnaire for me?

To keep our price down, we do not enter into bespoke contracts or fill out security checklists. However, we hope that our standard terms and conditions and this document include all the answers you need and cover all the events that you are concerned about and that you can use them to fill out whatever paperwork you require for your own systems.

If you have questions about our service that aren't covered here or aren't in our terms and conditions then do get in touch and, if we can, we will add the answers to this or our terms and conditions.

Do you offer a service level agreement?

To keep our price down, we do not. However, we take fulfilling our obligations to you very seriously and will do our upmost to ensure our service is there whenever you need it.

What happens if my account subscription should expire?

We want to avoid painful mistakes happening because, for instance, a subscription expires during a school holiday and nobody is around to pay the bill. So we do not immediately delete your data when your subscription expires unless you specifically ask us to.

However, after an account has been inactive for a significant time we will permanently delete your data.

Do you store data outside of the EU?

No.

What encryption principles are used for data in transit?

We regularly check our encryption meets modern standards and improve it as appropriate. At the moment we use a 2048 bit key, SHA256 with RSA and allow TLS1.0, TLS1.1, and TLS1.2. We are reviewing whether we should drop TLS 1.0 support.

What encryption key management processes are in place?

We use AWS to manage our encryption keys and provide them to authorised servers at the right moment.

The data centre hosting Tapestry is ISO 27001 accredited. Which version of ISO 27001 is it, and who is the accrediting company?

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

Do you follow standard X or have you been certified as Y?

Unless mentioned above, no. We take security very seriously and regularly review what we do. But we have not yet, for instance, undergone ISO27001 accreditation as a business.

Which board member is responsible for security?

Our Managing Director, Stephen Edwards, is responsible for security.

Do you have a documented framework for security governance, with policies governing key aspects of information security relevant to the service?

We do not yet have a complete set of documentation. We have started on the process of creating an ISO 27001 compliant documentation set, but the process is not yet complete.

Can you provide evidence that security and information security are part of your financial and operational risk reporting mechanisms, ensuring that the board would be kept informed of security and information risk?

We are a small firm so our board, Stephen Edwards and Helen Edwards, are closely involved in every decision taken by the firm.

We are very aware of the importance of information security. We discuss it in almost every meeting and we continuously attempt to improve our security.

We have a weekly formal review of our security state (see above)

We get independent penetration testers to review our system (see above)

Can you provide evidence of processes to identify and ensure compliance with applicable legal and regulatory requirements?

We discuss compliance in almost every meeting, particularly during this period of transition to the GDPR.

We have appointed a Data Protection Officer to hold us to account on this point.

Do you track the status, location and configuration of service components throughout their lifetime?

Yes. Our software configuration is managed under version control, with repeatable builds and change logging.

Yes. Our hardware configuration is managed under version control, with repeatable builds and change logging.

Do you assess changes to the service for potential security impact and monitor that impact to completion?

Yes.

How are potential new threats, vulnerabilities or exploitation techniques which could affect the service assessed?

We run regular automated tests and internal security reviews to examine the configuration and security of our servers.

We engage external penetration testers to assess our system against the latest threats.

Do we use relevant sources of information relating to threat, vulnerability and exploitation techniques, eg NIST, NCSC?

Yes. We monitor CVEs relating to the software our service depends on.

Yes. We regularly review guidance from the NCSC and OSWAP. We do not regularly review guidance from NIST.

How are known vulnerabilities prioritised and tracked until mitigations have been deployed?

We have automated notifications of vulnerabilities that are in our deployed code. These notifications are only quietened when fixes have been deployed.

We have internal issue tracking for required code and deployment changes.

We review and prioritise remaining security actions at least once a week.

What are the timescales for implementing mitigations? E.g. in patching policy?

This depends on the vulnerability.

For instance, if we believe the vulnerability could lead to data exposure, we would immediately take Tapestry offline while we fix the vulnerability. Because Tapestry would be offline, it would be our highest priority to fix. We have procedures for calling in engineers out of hours and at weekends. We have procedures for deploying changes to our production configuration within hours.

If the vulnerability was assessed as being of low risk, it would be deployed as part of our regular code and configuration updates. These tend to be made at least once every two weeks and are often made several times a week.

Other than for fault-finding, are activity logs monitored for suspicious activity, potential compromises or inappropriate use of the service?

Activity logs for our backend system have automated alerting for suspicious activity. These alerts are seen by all developers and by Stephen Edwards.

Activity logs for our customers are not monitored by us. They are available to customers to monitor.

Do we have an incident management process?

Yes. An incident will be uniquely identified and a named individual will be allocated responsibility for managing an incident through our support system. We have standard procedures for common incidents.

What is the process for the vendor to report incidents to the customer?

See “Keeping in touch about security” above.

Is 2-factor authentication available to end users?

No. But if sufficient numbers of users ask for it, we will implement it: Get in touch with us at customer.service@eyfs.info.

Which NSCC system architecture do you use?

Of the list at https://www.ncsc.gov.uk/guidance/systems-administration-architectures our system is closest to the 'bastion' model.

The service is run on partitioned and private networks. Management functions are carried out by devices on the corporate network which access to the private networks through bastions.

What provision is made for customers to access / monitor audit records for system / data access?

Customers have direct self-service access to logs that show changes to data.

We can provide logs of who has viewed data on request to customer.service@eyfs.info.

Changes to this document

18/Jan/2017 – Tom changed the certificate SHA1 fingerprint, since we have just deployed a new certificate to our servers with the eylj.org alternate domain name.

20/Feb/2017 – Emily changed the "Deleting Data When No Longer Needed" to say that children will by default be kept for 90 days, rather than 30 days, before permanent deletion. The change in policy was due to nursery staff frequently deleting children at the end of the Summer term, but then unexpectedly needing the data at the start of Autumn term.

11/April/2017 – Tom made it explicit that you can instruct us to delete all your data immediately, at an any time. Tom also shortened the wording on "What happens if my account subscription should expire" without changing the meaning.

15/June/2017 - Tom clarified: 1) backups are, like the primary data, encrypted and stored in data centres with the same level of physical security; 2) Unless otherwise mentioned, we do not have a particular security standard; 3) We will delete backups of data if you request us to; 4) how you get in touch with us, how we can get in touch with you.

5/October/2017 - Tom converted the document into Markdown and fixed the styling. No changes in content.

28/November/2017

- Tom added to the FAQ section in response to queries from Tameside
- Tom added "Steve is the board member responsible for security."

29/November/2017

- Tom added a section on what we are doing for GDPR compliance.