Draft Contract for the Tapestry Online Learning journal

Foundation Stage Forum Ltd

5 January 2018

Contents

A note on this draft

This is an early draft of a new contract between the Foundation Stage Forum Ltd and our customers who use Tapestry.

We aren't trying to change anything fundamental about our relationship and what we do for you. But we are trying to:

1. Improve the clarity of the contract.
2. Make it unambiguously clear how we work together to ensure we are compliant with the forthcoming changes to data protection law in the EU (known as the GDPR).

This is not the final contract. It is a draft and we would like your feedback in order to make it better for all our customers. Please send your thoughts to contract-feedback@eyfs.info.

The goal is to agree an updated contract with all our customers by the end of March 2017.

Your contract with us for the use of Tapestry

1. We are the Foundation Stage Forum Ltd, a company registered in England with company number 05757213 and a registered address of 1, Southdown Avenue, Lewes BN7 1EL, UK.
2. You are a childminder, educator, nursery, school or similar educational organisation.

What you get

3. This contract is for a 12 month subscription to Tapestry, our online learning journal, together with:
   - Our tutorials
   - Email support during UK business hours
   - Access to the https://eyfs.info discussion forum

What you do not get

4. We do not provide telephone or face to face support.
5. We do not provide direct support to any relatives that you add to Tapestry. If they contact us, we will usually direct them back to you. We do this because it is difficult for us to know whether their requests are authorised by you.
6. We do our best to provide Tapestry at all times (see our Annex B: Tapestry Security), but we cannot guarantee this.

Tapestry, our online learning journal

7. You must be the Data Controller of the information that you enter into Tapestry (as you are for your paper records), we will be the Data Processor. If you don't know what those terms mean, it is essential that you find out. A starting point for finding out is https://ico.org.uk.
8. You agree with our approach to data protection, privacy and security and to do your part. We describe our approach and what we expect of you in these linked annexes:
   - Annex A: Tapestry Data Protection
   - Annex B: Tapestry Security
   - Annex C: Tapestry Privacy
9. You agree to our current sub-processors:
   - Annex D: Tapestry Sub-processors
10. We will help you to comply with your duties under UK data protection legislation. In most cases you can use the tools we provide. If you ask us for extra help in complying we will give it to you, but we may charge you

our costs in helping. More detail is provided in Annex A: Tapestry Data Protection.

11. If you wish to audit us under UK data protection legislation, you may do so, but we may charge you our costs in participating in your audit.

Our tutorials

12. You may copy, store, share and adapt our tutorials for the purpose of making better use of Tapestry.

Our Billing and Support System

13. If you contact us by email or through our websites then we will store and process the information you provide in our billing and support system. Unlike the data you enter into Tapestry, we are the Data Controller for information in our billing and support system. We describe how we use that data in Annex E: Billing and support data.

Our Discussion Forum

14. You do not need to use our discussion forum. But if you choose to, then you agree to the conditions set out in Annex F: Use of our discussion forum.

Fees

15. You must pay our fee in full before we will start your Tapestry subscription
16. Our fee, as set out on our website, is based on the maximum number of children you wish to have in your Tapestry account during the 12 month subscription.
17. You can add or remove individual children throughout the year so long as the maximum number of children is not exceeded at any one moment.
18. If you have not paid your fee in full then:

- we may not provide access to Tapestry.
- after 90 days, we will delete the data that you have entered into Tapestry.

19. If you wish to increase the maximum number of children you can have in your Tapestry account during the 12 month subscription then we will charge you the difference between what you have paid and the current fee for an account with the increased number of children. This will not extend your subscription.

20. You must pay us UK Pounds Sterling including any applicable VAT. If you choose to pay by bank transfer you must bear all currency conversion and bank transfer costs.

Termination

21. You can stop using Tapestry at any time and ask us to return and / or delete the data you have entered into Tapestry, but we will not refund any fees that you have paid unless:
    - You are within the first month of your Tapestry subscription
    - We materially change this contract to your detriment
22. We may, after discussing the situation with you, stop providing you with Tapestry if you:
    - misuse our systems or
    - create an unreasonable load on our systems or
    - cause us unreasonable costs or
    - abuse our staff or
    - breach this contract.

Changes and disputes

23. If something goes wrong, our total liability to you is limited to the annual fee that you have paid us for Tapestry.
24. Our contract with you is under English law and any dispute will be settled by an English court.
25. This document, together with its annexes are our entire contract with you. If you want to vary this contract, or add additional terms, then there will need to be written and explicit agreement between you and one of our company directors. To keep our costs and prices down, we rarely do this. In particular, unless explicitly agreed to by one of our company directors, we do not accept any standard purchasing terms and conditions that you may usually apply.
26. We may change this contract, but will give you reasonable warning.

Annex A: Tapestry Data Protection

We are the Foundation Stage Forum Ltd, a company registered in England with company number 05757213 and a registered address of 1, Southdown Avenue, Lewes BN7 1EL, UK.

You are a childminder, educator, nursery, school or similar educational organisation.

This Annex relates to the use of Tapestry, our online learning journal. Annex E relates to data in our billing and support system. Annex F relates to data in our discussion forum.

We need to work together to ensure we are compliant with data protection regulations when using Tapestry.

This annex should be read in conjunction with our overall contract and, in particular, Annex B which explaining our approach to security and Annex D which lists our sub processors.

Our jurisdiction

We are headquartered in the UK. This contract is under UK law.

Our lead supervisory authority for data protection is the UK Information Commissioner's Office (https://ico.org.uk).

Where is data stored?

Our processing and storage of your data happens within the EU.

The primary processing and storage location is in Ireland.

Our offsite backups are stored in Germany.

What data is placed into Tapestry?

You are in control of the data you put into Tapestry. You choose what to add, you choose what is done with it and who it is shared with. You can always access, correct and delete the data.

When you use Tapestry:

1. You enter data about the children in your care, their progress and their welfare. You choose which children and what data.
2. You can, optionally, analyse and monitor the children's progress and welfare.

3. You can, optionally, share the data about the children with others that you choose, such as a child's relatives.
4. You can add text and, optionally, pictures and videos.
5. You can choose when and what data to delete.
6. You can correct any data that you enter.

Who is responsible for what?

The first thing to agree is that:

1. You are the data controller for data you, or the people you give access, add to Tapestry.
2. We are the data processor.

If you don't know what those terms mean, it is *essential* that you find out. A starting point for finding out is https://ico.org.uk.

You must:

- Have a lawful basis for entering data into Tapestry.
- Use Tapestry in a way that is compliant with data protection law.
- Respond to data protection requests.
- Keep your contact details on Tapestry up to date.

We must:

- Only process data on your instructions.
- Ensure that people we use to process your data are subject to a duty of confidence.
- Take appropriate measures to ensure the security of our processing.
- Only engage sub-processors with your prior consent.
- Assist you in providing subject access and allowing data subjects to exercise their rights under data protection law.
- Assist you in meeting your legal data protection obligations in relation to:
  - the security of processing
  - the notification of personal data breaches
  - and data protection impact assessments
- Delete or return all personal data to you as requested at the end of the contract.
- Submit to your audits and inspections.
- Provide you with the information to meet your legal obligations.
- Tell you immediately if we are asked to do something infringing data protection law.

What we expect of you

You must have a lawful basis for putting data into Tapestry

We rely on you to ensure you have a lawful basis for putting data into Tapestry. If you haven't worked out what your lawful basis is, please do so immediately. Once again, the UK Information Commissioners Office, https://ico.org.uk, is a good starting point.

If you are relying on consent as your lawful basis, then we rely on you to have gained the consent for whatever data you intend to put on Tapestry and to remove data if consent is later withdrawn.

You must use Tapestry in a way that is compliant with data protection law

As the controller of the data you put in Tapestry, you must comply with data protection law. This includes ensuring that the data is:

1. Processed lawfully, fairly and in a transparent manner in relation to individuals.
2. Collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall not be considered to be incompatible with the initial purposes.
3. Adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed.
4. Accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay.
5. Kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes subject to implementation of the appropriate technical and organisational measures required by the GDPR in order to safeguard the rights and freedoms of individuals.
6. Processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.

Source: https://ico.org.uk/for-organisations/data-protection-reform/overview-of-the-gdpr/principles/

We will do our part in helping you to comply (described below).

You must respond to data protection requests

Using Tapestry normally involves processing data about people (children, possibly staff, possibly relatives). Those people have rights under data protection law, including:

1. The right to be informed
2. The right of access
3. The right to rectification
4. The right to erasure
5. The right to restrict processing
6. The right to data portability
7. The right to object
8. Rights in relation to automated decision making and profiling

Source: https://ico.org.uk/for-organisations/data-protection-reform/overview-of-the-gdpr/individuals-rights/

You are responsible for responding to those requests. We have designed our system to help you to respond.

You must keep your contact details on Tapestry up to date

You must keep your contact details up to date within Tapestry. We use these to:

1. Contact you
2. Verify that instructions we receive come from you

If they are not up to date, you may not receive our messages.

In particular, we sometimes receive requests from customers stating that the only manager registered on a school, childminder or nursery's Tapestry account has left, and requesting that the ownership be transferred to a new person. In order to verify that the request is legitimate we have to take several steps. Even if these steps are successful, they may mean a delay of weeks during which time Tapestry may not be accessible by you. To avoid this, please ensure you update contact details before a manager departs and, ideally, always register more than one manager on the Tapestry system.

What you can expect of us

We will only process data on your instructions

Tapestry only does what you tell it. We do not do any processing that you do not tell us to do.

To be absolutely clear: we don't own your data; we don't sell your data; we don't use your data for advertising; we don't pass on your data except when you instruct us to.

You can add users to Tapestry who can then also instruct Tapestry. You can adjust what data those users see and what they can do with the data.

If you have been told to restrict processing of someone's data, then you are responsible for not using Tapestry to do any further processing of that person's data. You are responsible for ensuring any users that you have added to Tapestry do no further processing. The easiest way to do that is to use Tapestry to mark the child or user as inactive.

We will ensure that people we use to process your data are subject to a duty of confidence

Our staff who process your data are:

1. Contractually bound to keep your data confidential.
2. Vetted by us. This includes a DBS check, which is updated annually.

We will take appropriate measures to ensure the security of our processing

The measures we take are described in Annex B.

We have started the process of becoming certified as ISO 27001 compliant. When we have become certified we will update this contract to confirm that we are.

We will engage sub-processors only with your prior consent

Our sub-processors, and what they do, are described in Annex D. We will email you in advance of any changes to give you time to object.

Any sub-processors we use are always under a written contract and are always bound to keep your data confidential.

We will assist you in providing subject access and allowing data subjects to exercise their rights under data protection law

You can download all the information that has been entered into Tapestry.

[NOT YET IMPLEMENTED: We provide a section in the control panel where you can download a single file that brings together all the information Tapestry holds about a particular child or a particular user.]

You can correct all the information that has been entered into Tapestry.

You can delete all the information that you have entered into Tapestry.

We will assist you in meeting your legal data protection obligations

The security of processing

We describe our current security approach in Annex B.

If you believe that there is something that should be described in Annex B but is not, please let us know.

If you wish us to describe our security in a particular way (such as by filling out forms for you) then we may pass on our costs in doing so.

We do not usually implement bespoke security measures. However, we are always interested in improving our service, so please do let us know of anything that you would like to see.

Notification of personal data breaches

If there is a personal data breach, we will:

1. Help you to work out who has been affected.
2. Help you to work out what data may have been breached.
3. Help you to determine the cause of the breach.
4. Help you in your dealing with the Information Commissioners Office.

The Information Commissioners Office require notification of any data breach that is "likely to result in a risk to the rights and freedoms of individuals" within 72 hours of you or us becoming aware of it. We will prioritise our work to meet that deadline.

If you wish us to go further than that, we will do our best but may have to pass on our costs in helping you.

Data protection impact assessments

We cannot carry out a data protection impact assessment for you, because we do not know what data you intend to place in Tapestry.

[NOT YET IMPLEMENTED We do provide some example documents on risks that you can customise when carrying out your own assessments.]

If you wish us to go further than that, we will do our best but may have to pass on our costs in helping you.

We will delete or return all personal data to you as requested at the end of the contract

You can delete data at any time. You can download data at any time.

At the end of the contract our standard practice is to delete your data from our systems after 90 days. The data will be deleted from our backup systems 90 days after it is deleted from our systems. We are happy to delete your data sooner if you ask us to.

We are happy to return your data to you at any time. If you want your data in a particular format, we will do our best, but may have to pass on our costs in providing it to you in that format.

We will submit to your audits and inspections

We provide our approach to security in Annex B for you to audit.

We have started the process of becoming ISO 27001 certified. When we have done so, we will update this contract and provide you with access to the certification for you to audit.

If you want to submit us to further audit or inspection, we will do our best to help you, but may have to pass on our costs in complying with your request.

We will provide you with the information to meet your legal obligations

We believe this contract and its annexes, combined with the tools provided within Tapestry, provide you with what you need to meet your legal obligations. If you think there is something missing, please let us know.

If you have a specific or unusual request for information, we will do our best to help you, but may have to pass on our costs in complying with your request.

We will tell you immediately if we are asked to do something infringing data protection law

If we are asked to do something that we believe infringes data protection law we will not do so, and we will try and reach you through the contact details you

have given us to explain what has happened.

If something goes wrong

Complaints

If you have a complaint, then please contact us at customer.service@eyfs.info

Our Data Protection Officer

If you have a concern that we have not addressed, please contact our Data Protection Officer:

Lauren Foley dpo@eyfs.info 1 Southdown Avenue Lewes BN7 1EL UK

Annex B: Tapestry Security

This annex relates to the use of Tapestry, our online learning journal. Annex E relates to data in our billing and support system. Annex F relates to data in our discussion forum.

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. This annex 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 annex explains what we do and what we hope you will do.

The latest copy of this annex, 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., an early years organisation that has provided resources and support for the early years workforce since February 2003. We have contracts with many local authorities, some 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.

We have two directors: Helen and Stephen Edwards.

Director: 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. 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.

Director: 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.

Data Protection Officer: Lauren Foley

Lauren Foley is our Data Protection Officer. Her direct email is dpo@eyfs.info.

Lauren joined the Foundation Stage Forum in 2014 after graduating from the University of Birmingham. She was designated our data protection officer after completing GDPR training in November 2017.

Data Protection Law

We are compliant with UK data protection law. We describe our approach to data protection in Annex A.

To summarise it in brief: 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 data without your permission.

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

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 delay the deletion for 90 days 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.

Data will remain in our backups for 90 further days. 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

ISO 27001

We are working towards becoming independently certified as ISO 27001 complaint. When we have achieved certification we will update this contract and provide you with access to the certification.

Our data center, Amazon Web Services, has been independently certified as ISO 27001 compliant.

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 access to your data.

It is important that you think about your procedures for what sort of data you put on Tapestry 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 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 10 characters and we allow and encourage you to set a tougher standard than that (by, for instance, requiring longer passwords).

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 discourage this. We prefer you to use the option of sending reset links that allow users to set their own passwords and PIN.

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 add an email address for the new manager. In order to verify that the request is legitimate we have to take several steps. Even if these steps are successful, they may mean a delay of weeks during which time Tapestry may not be accessible by you. To avoid this, please ensure you update contact details before a manager departs and, ideally, always register more than one manager on the Tapestry system.

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 your 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 devices may have copies of the pictures and videos that have been taken outside of the app. There is also a setting that allows copies of pictures and videos taken within the app to be stored in the device's picture gallery. However, by default this setting is disabled. 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 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 check was in August 2017. 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 primary physical locations are in the Republic of Ireland, the backup physical locations are in Germany).

These backups should be, at most, 24 hours old and we should have 90 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).

Please note that backups are for disaster recovery. We will use them to restore your data should it become lost or corrupted on the live system. It is not designed for easy access to restore specific bits of data that you have deliberately deleted

from the live system. If you ask us to retrieve specific bits of information from the backups, we will do so, but we may need to charge our costs.

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 security 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 contract, including its annexes, 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 then do get in touch and, if we can, we will add the answers to this contract.

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 utmost 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, 90 days after your subscription expires we will permanently delete your data. Data will remain in our backups for 90 further days.

If you wish, you can instruct us to to delete all your data sooner.

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 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.

Annex C: Tapestry Privacy

This annex describes our privacy policy for people who access the Tapestry online learning journal service, (https://tapestryjournal.com).

This policy is intended to be shared with any person who uses Tapestry.

We are the Foundation Stage Forum Ltd, a company registered in England with company number 05757213 and a registered address of 1, Southdown Avenue, Lewes BN7 1EL, UK.

Our customers are childminders, educators, nurseries, schools or similar educational organisations.

You are someone who has been given access to Tapestry by one of our customers.

You may have rights under EU Data Protection legislation relating to information we store about you. These rights are described here: https://ico.org.uk/for-the-public/. If you want to exercise those rights, please contact the customer who is storing data in Tapestry in the first instance (e.g., the school or nursery). If they want help in carrying out your request, they can contact us.

Our lead supervisory authority for data protection is the UK Information Commissioner's Office (https://ico.org.uk).

The Service

Our customers pay us to provide them with a service that allows them to create online learning journals for children under their care, monitor those children's progress and share this information with their staff and, if they wish, those children's parents and relatives.

What data do we collect?

Our customers may choose to store some of the following data on our service:

- The names and email addresses of their staff
- The names, dates of birth and postcode of their children
- The names and email addresses of the parents and relatives of their children
- The contents of a learning journal:
  - assessments of children's performance
  - notes, photographs and videos of the children
- A record of the child's care:
  - what they ate and drank
  - toileting
  - how they slept
  - whether they had any accidents

Our customers store this information in order to record, analyse and, if they wish, share the progress of their children.

Our customers have the freedom to choose what data they store and who they store it about.

Our customers choose who has access to the data.

Our customers are able to correct and delete data at will.

If you wish to know the policy for exactly what data is stored in Tapestry about a specific person and who it is shared with, please contact the relevant childminder, educator, nursery, school or similar educational organisation.

In providing the service, we will send automated emails to staff and parents in order to confirm email addresses, reset passwords and notify them of events relating to the customer (such as when a new observation is added about a child). We never send any marketing information, though we do send staff a newsletter about Tapestry.

We ONLY access the data stored by our customers in order to carry out our customer's instructions, to maintain or improve the service or to fix faults. We do not use our customer's data for marketing. We use sub-contractors to process some of the data, but we do not otherwise share this data with other organisations.

When you visit the Tapestry web site we collect your:

- IP address
- Information your computer sends about its web browser and operating system
- What pages you look at (e.g., the list of observations), but not the content of those pages (i.e., we could not tell directly from the data whether the list of observations contained information about a particular child, though given time and access to the data above it would be possible to figure that out)

We use this information to monitor the security of our service, to help us figure out how to improve the service (e.g., what browsers should we support? How much capacity should we add?) and to improve the way we market the service (e.g., what search terms were used to discover our site).

If you use our phone or tablet application we collect:

- The make and model of your phone or tablet
- The version of your phone or tablet's operating system
- Details of any crashes that occur in the application
- What screens you look at in the application (e.g., the list of observations), but not the content of those screens (i.e., we could not tell directly from the data whether the list of observations contained information about a

particular child, though given time and access to the data above it would be possible to figure that out)

We use this information to monitor the security of our service and to to help us figure out how to improve the service (e.g., what causes crashes? which crashes need fixing most urgently?)

Who owns the data?

Our customers own the data they place in our service. We do not. Formally, in UK data protection legislation terms, our customers are the "Data Controller" and we are the "Data Processor".

There are three exceptions to this, where we are the "Data Controller":

1. The content of our billing system
2. The content of our support ticket system
3. The content of our forums

These exceptions are described in more detail in Annex E and Annex F.

Who do we share data with?

We do not share data, except as explicitly requested by our customers.

If they wished, our customers might give other people (e.g., staff or parents) access to data. They might download or print some or all of the data and share it with other people (e.g., staff, parents, the government). They might transfer some of the data to another organisation (e.g., parents, the government, another educational establishment looking after a child).

We ONLY access the data stored by our customers in order to carry out our customer's instructions, to maintain or improve the service, or to fix faults.

How do we collect the data?

Most data is entered by our customers directly into our website or through our phone and tablet applications. Our customers may, if they wish, permit parents and relatives of children to add data to the service.

Some data (described above) is sent automatically by your web browser or by our applications.

We may store cookies on your computer in order to verify that you are logged in and to store your preferences. The cookies themselves do not contain any identifiable information about you or about what you look at.

Can I see my data that is stored on your system?

Yes. The school, childminder, nursery or similar educational organisation, can give you a copy of data about you that they or you have stored in Tapestry. We can provide you with a copy of any of the other data that has been collected (e.g., our records of your IP address and / or make and model of your tablets etc.).

Can I have my data corrected or deleted?

Yes. The school, childminder, nursery or similar educational organisation, can correct or delete the data they or you have stored in Tapestry.

The process of deletion is gradual: initially deleted data is moved to a 'deleted' area in case it was deleted in error. After a delay, it is then permanently deleted from our main systems. After a further delay, it is then permanently deleted from our backups.

What are our customer's responsibilities?

Our customers decide who to add data about, what data to add, and how long to keep it for. They have overall responsibility for complying with Data Protection law (or the equivalent in other countries).

We describe this in more detail in the contract we have with our customers. But, for instance, they have to:

- Ensure they have a legal basis for what data they store on Tapestry and who they share it with.
- Think about what information it is appropriate to share with whom, given their situation and that of the children under their care.
- Respond to requests for access to data.
- Train their staff about sensible security and confidentiality precautions:
  - Taking care of passwords.
  - Taking care not to install software on computers that may compromise security.
  - Taking care not to access material from inappropriate places where it can't be kept appropriately confidential.
- Delete data when it is no longer required.
- Remove access for people who no longer need access.
- Give parents instructions in accordance with their safeguarding policy.

Contacting Us

You can contact us at customer.service@eyfs.info or 1, Southdown Avenue, Lewes BN7 1EL, UK.

We also have a Data Protection Officer, Lauren Foley, who can be reached at dpo@eyfs.info.

Annex D: Tapestry Sub-processors

To continue to use Tapestry, we require your consent to our use of the following sub-processors:

- Amazon Web Services - They host Tapestry. They are ISO 27001 compliant.

[NOTE: We currently also use the following suppliers, but are in the process of removing them either by replacing their service with that of Amazon Web Services or bringing the service in house].

- Viper - Manage our laptops and telephones
- Mailchimp - Manage some of our outbound email.
- Sparkpost - Manage some of our outbound email.
- Crashlytics - Manage some of our crash reporting on our Android, iOS and Amazon Fire apps.

Annex E: Billing and support data

1. We are the Foundation Stage Forum Ltd, a company registered in England with company number 05757213 and a registered address of 1, Southdown Avenue, Lewes BN7 1EL, UK.
2. You are a childminder, educator, nursery, school or similar educational organisation.
3. This annex relate to data in our billing and support system. It does not relate to data placed in the Tapestry online learning journal (see Annex A) or to data placed in our discussion forums (see Annex F).

What data do we collect?

3. We collect the following information about people who contact us by email or through our support ticket system:

- The person's email address and the contents of the email

4. If you contact us by telephone, post or face-to-face we may also keep notes of those interactions.
5. We store:

- Your name, email address, telephone number and postal address
- The name, email address and telephone numbers of anyone you tell us who administers or pays for your account with us.

6. Credit card payment information is given directly to a payment service provider. We do not hold any credit card information ourselves.

Why do you need this data?

7. We need this data to:

- Charge you for our service
- Respond to questions or problems raised by you
- Contact you if we have questions about your account
- Decide what changes to make to our service

Who do you share this data with?

8. We make use of subcontractors to provide our service to you and they may see some or all of this data:

- Amazon Web Services - For hosting.

- United Hosting - For hosting.
- Barnian Media Ltd - For technical support.
- SagePay - For managing credit card payments.
- Fastmail - For managing our email

9. We do not use or share your data for any reason other than to provide our service to you. For the avoidance of doubt: we do not sell your data.

Where is the data stored?

10. Your data is stored within the EU. Our processing is carried out within the EU.

How long do you keep this data?

11. We keep your data for up to 7 years. We keep data this long in case it is required in an audit and to help us decide what changes to make to our service.

How do I exercise my rights under data protection law?

12. We are the data controller of this data.
13. Your rights under data protection law are described at https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/individual-rights/. They include the right to see and correct this data.
14. To exercise those rights, contact us at customer.service@eyfs.info
15. We also have a Data Protection Officer, Lauren Foley, who can be reached at dpo@eyfs.info
16. Our lead supervisory authority for data protection is the UK Information Commissioner's Office (https://ico.org.uk).

Annex F: Use of our discussion forum

1. We are the Foundation Stage Forum Ltd, a company registered in England with company number 05757213 and a registered address of 1, Southdown Avenue, Lewes BN7 1EL, UK.
2. You are a childminder, educator, nursery, school or similar educational organisation.
3. We have a discussion forum (https://eyfs.info) that you may use to discuss issues facing childminders, educators, nurseries, schools or similar educational organisations.

Liability

4. We do not vouch for the accuracy, completeness or usefulness of any material on the forum. Use it at your own risk.
5. The material express the views of the author of the material, and not necessarily our views.
6. If you feel any material on the forum is is objectionable, please contact us immediately at customer.service@eyfs.info.

Content and ownership of your messages

6. Don't post anything we won't like.
    - We like professional discussion of the issues facing issues facing childminders, educators, nurseries, schools or similar educational organisations.
    - We don't like things that are unkind, illegal, lies, use language you wouldn't want children to hear, or are shameless advertising.
7. Don't post anything that you don't have permission to post. For instance, if you didn't write the material you are posting, make sure you have the permission of the person who wrote it *before* you post it.
8. On shameless advertising: Occasionally during the course of a discussion it may be appropriate for a you to mention a product or service with which you are involved if it helps the discussion and doesn't annoy anyone. We will use our discretion in those cases.
9. If we don't like what you post, or fear you may not have permission to post it, we will remove it.
10. If we keep having to remove your material, or if we *really* don't like it, we will bar you from the forum.
11. When you post material, you retain copyright but grant us the right to use the material:

- without payment,
- in any way we choose,
- anywhere in the world,
- forever.

12. If we use your material, we will try to attribute it to you.

13. If you wish to copy material posted by someone else, please contact us or the person who posted for permission.

Privacy and Data Protection

14. We store any data that you submit to us, plus your IP address, details about your browser and computer and which pages on our site you view.

15. We store and process this data in order to:

    - provide a discussion forum,
    - monitor abuse,
    - fix bugs
    - and to improve our service.

16. Your data is stored within the EU. Our processing is carried out within the EU. Our forum is accessible from outside of the EU, so material you post may be viewed from outside of the EU.

17. Your forum account will lapse once your Tapestry subscription lapses or, if you have a separate forum subscription directly or through your local authority, once that subscription lapses.

18. When your forum account lapses you will no longer be able to log into the forum or post material to the forum. At our discretion, the material you have posted may remain on the forum.

19. When your forum account has lapsed we will only use the personal information that you have provided us to:

    - help you re-activate your forum account if you later wish to re-subscribe
    - keep track of who posted what material in case we need to attribute it to you or in case we need to verify that you had permission to post the material.

20. We will delete the personal information that you have provided us at most 7 years after your forum account has lapsed. At our discretion, the material you have posted may remain on the forum.

21. We are the data controller for this data. To exercise your rights under UK data protection law you can contact us at customer.service@eyfs.info

22. We have a Data Protection Officer, Lauren Foley, who can be reached at dpo@eyfs.info

23. Our lead supervisory authority for data protection is the UK Information Commissioner's Office (https://ico.org.uk).