

1 Contract for the Tapestry Online Learning  
2 Journal

3 Foundation Stage Forum Ltd

4 1 May 2018

5 **Contents**

6 **A note on this contract** **6**

7 **Your contract with us for the use of Tapestry** **7**

8 What you get . . . . . 7

9 What you do not get . . . . . 7

10 Tapestry, our online learning journal . . . . . 7

11 Our tutorials . . . . . 8

12 Our Billing and Support System . . . . . 8

13 Our Discussion Forum . . . . . 8

14 Fees . . . . . 8

15 Termination . . . . . 9

16 Changes and disputes . . . . . 9

17 **Annex A: Tapestry Data Protection** **10**

18 The legally required terms in a Data Processing Agreement or Contract 10

19 Our jurisdiction . . . . . 11

20 Where is data stored? . . . . . 11

21 What data is placed into Tapestry? . . . . . 12

22 Who is responsible for what? . . . . . 12

23 What we expect of you . . . . . 13

24 You must have a lawful basis for putting data into Tapestry . . . 13

25 You must use Tapestry in a way that is compliant with data  
26 protection law . . . . . 13

27 You must respond to data protection requests . . . . . 14

28 You must keep your contact details on Tapestry up to date . . . 15

29 What you can expect of us . . . . . 15

30 We will only process data on your written instructions . . . . . 15

31 We will ensure that people we use to process your data are subject  
32 to a duty of confidence . . . . . 17

33	We will take appropriate measures to ensure the security of our	
34	processing . . . . .	17
35	We will engage sub-processors only with your prior consent . . . .	17
36	We will assist you in providing subject access and allowing data	
37	subjects to exercise their rights under data protection law	18
38	We will assist you in meeting your legal data protection obligations	18
39	We will delete or return all personal data to you as requested at	
40	the end of the contract . . . . .	19
41	We will submit to your audits and inspections . . . . .	19
42	We will provide you with the information to meet your legal	
43	obligations . . . . .	19
44	We will tell you if we become aware of a data breach . . . . .	20
45	We will tell you immediately if we are asked to do something	
46	infringing data protection law . . . . .	20
47	If something goes wrong . . . . .	20
48	Complaints . . . . .	20
49	Our Data Protection Officer . . . . .	20
50	<b>Frequently Asked Questions</b>	<b>21</b>
51	With regard to Brexit: will the data be hosted and backed up in the	
52	UK once Brexit is finalised? . . . . .	21
53	<b>Annex B: Tapestry Security</b>	<b>22</b>
54	Security Responsibilities . . . . .	22
55	Who are we? . . . . .	22
56	The Foundation Stage Forum Ltd . . . . .	22
57	Director: Stephen Edwards MSc . . . . .	23
58	Director: Helen Edwards DPhil . . . . .	23
59	Data Protection Officer: Lauren Foley . . . . .	23
60	Data Protection Law . . . . .	23
61	Access to data . . . . .	24
62	Deleting data when it is no longer needed . . . . .	24
63	Organisational data security . . . . .	25
64	ISO 27001 . . . . .	25
65	Staff . . . . .	25
66	Procedures . . . . .	26
67	Passwords . . . . .	26
68	Technical data security . . . . .	27
69	Physical security . . . . .	28
70	Software security . . . . .	29
71	Encryption . . . . .	29
72	Partitioning . . . . .	30
73	Logging . . . . .	30
74	Verification (also known as Penetration Testing) . . . . .	30
75	Capacity, Redundancy and Backups . . . . .	31
76	Keeping in touch about security . . . . .	31

77	Frequently asked security questions . . . . .	32
78	Can you fill out this security questionnaire for me? . . . . .	32
79	Do you offer a service level agreement? . . . . .	32
80	Are you insured? . . . . .	32
81	What happens if my account subscription should expire? . . . . .	32
82	Do you store data outside of the EU? . . . . .	33
83	What encryption principles are used for data in transit? . . . . .	33
84	Have you disabled TLS 1.0 support? . . . . .	33
85	What encryption key management processes are in place? . . . . .	33
86	The data centre hosting Tapestry is ISO 27001 accredited. Which	
87	version of ISO 27001 is it, and who is the accrediting	
88	company? . . . . .	33
89	Do you follow any other standards or hold any other certifications? . . . . .	33
90	Which board member is responsible for security? . . . . .	33
91	Do you have a documented framework for security governance,	
92	with policies governing key aspects of information security	
93	relevant to the service? . . . . .	34
94	Can you provide evidence that security and information security	
95	are part of your financial and operational risk reporting	
96	mechanisms, ensuring that the board would be kept in-	
97	formed of security and information risk? . . . . .	34
98	Can you provide evidence of processes to identify and ensure com-	
99	pliance with applicable legal and regulatory requirements? . . . . .	34
100	Do you track the status, location and configuration of service	
101	components throughout their lifetime? . . . . .	34
102	Do you assess changes to the service for potential security impact	
103	and monitor that impact to completion? . . . . .	34
104	How are potential new threats, vulnerabilities or exploitation	
105	techniques which could affect the service assessed? . . . . .	35
106	Do we use relevant sources of information relating to threat,	
107	vulnerability and exploitation techniques, eg NIST, NCSC? . . . . .	35
108	How are known vulnerabilities prioritised and tracked until miti-	
109	gations have been deployed? . . . . .	35
110	What are the timescales for implementing mitigations? E.g. in	
111	patching policy? . . . . .	35
112	Other than for fault-finding, are activity logs monitored for suspi-	
113	cious activity, potential compromises or inappropriate use	
114	of the service? . . . . .	36
115	Do we have an incident management process? . . . . .	36
116	What is the process for the vendor to report incidents to the	
117	customer? . . . . .	36
118	Is 2-factor authentication (2FA) available to end users? . . . . .	36
119	Can we require passwords to be changed every X days? . . . . .	36
120	Which NSCC system architecture do you use? . . . . .	36
121	What provision is made for customers to access / monitor audit	
122	records for system / data access? . . . . .	37

123	Does your organisation have differentiated access to data depend-	
124	ing on the sensitivity level? . . . . .	37
125	<b>Annex C: Tapestry Privacy</b>	<b>38</b>
126	The Service . . . . .	38
127	What data do we collect? . . . . .	38
128	What is the lawful basis for storing this data . . . . .	40
129	Whose data is it? . . . . .	40
130	Who do we share data with? . . . . .	40
131	How do we collect the data? . . . . .	41
132	Can I see my data that is stored on your system? . . . . .	41
133	Can I have my data corrected or deleted? . . . . .	41
134	What are our customer’s responsibilities? . . . . .	41
135	Contacting Us . . . . .	42
136	<b>Annex D: Tapestry Sub-processors</b>	<b>43</b>
137	List of sub-processors . . . . .	43
138	Changes to sub-processors . . . . .	43
139	<b>Annex E: Billing and support data</b>	<b>44</b>
140	What data do we collect? . . . . .	44
141	Why do you need this data? . . . . .	44
142	Who do you share this data with? . . . . .	44
143	Where is the data stored? . . . . .	45
144	How long do you keep this data? . . . . .	45
145	How do I exercise my rights under data protection law? . . . . .	45
146	<b>Annex F: Use of our discussion forum</b>	<b>46</b>
147	Liability . . . . .	46
148	Content and ownership of your messages . . . . .	46
149	Privacy and Data Protection . . . . .	47
150	<b>Changes to this contract</b>	<b>49</b>
151	2018 May 1 . . . . .	49
152	Tapestry Data Protection . . . . .	49
153	Tapestry Security . . . . .	49
154	Tapestry Privacy . . . . .	50
155	Tapestry Sub Processor . . . . .	50
156	2018 March 12 (Second Draft) . . . . .	50
157	Across all sections . . . . .	50
158	A note on this draft . . . . .	50
159	Overview . . . . .	50
160	Annex A: Tapestry Data Protection . . . . .	50
161	Annex B: Tapestry Security . . . . .	51
162	Annex C: Tapestry Privacy . . . . .	52
163	Annex D: Tapestry Sub-processors . . . . .	52

164	Annex E: Billing and support data . . . . .	52
165	Annex F: Use of our discussion forum . . . . .	52
166	2018 January 5 (First draft) . . . . .	52

167 **A note on this contract**

168 This is the new contract between the Foundation Stage Forum Ltd and our  
169 customers who use Tapestry. If you have read a previous draft, you can see a  
170 list of changes at the end of this document, or a version with “Track Changes”  
171 at <https://tapestry.info/draft-contract>.

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

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

178 You will be asked to agree to this contract through the Tapestry Control Panel.

## 179 **Your contract with us for the use of Tapestry**

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

## 185 **What you get**

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

## 191 **What you do not get**

- 192 4. We do not provide telephone or face to face support. However, at our  
193 discretion, we may offer to call you if we feel a query could be better  
194 resolved over the phone. We also do offer bookable telephone support  
195 sessions for a fee.
- 196 5. We do not provide direct support to any relatives that you add to Tapestry.  
197 If they contact us, we will usually direct them back to you. We do this  
198 because it is difficult for us to know whether their requests are authorised  
199 by you.
- 200 6. We do our best to provide Tapestry at all times (see our Annex B: Tapestry  
201 Security), but we cannot guarantee this.

## 202 **Tapestry, our online learning journal**

- 203 7. You must be the Data Controller of the information that you enter into  
204 Tapestry (as you are for your paper records); we will be the Data Processor.  
205 If you don't know what those terms mean, it is essential that you find out.  
206 A starting point for finding out is <https://ico.org.uk>.
- 207 8. You agree with our approach to data protection, privacy and security and  
208 to do your part. We describe our approach and what we expect of you in  
209 these linked annexes:
  - 210 • Annex A: Tapestry Data Protection
  - 211 • Annex B: Tapestry Security
  - 212 • Annex C: Tapestry Privacy
- 213 9. You agree to our current sub-processors:
  - 214 • Annex D: Tapestry Sub-processors

- 215 10. We are compliant with UK data protection legislation (sometimes referred  
216 to as the ‘GDPR’).
- 217 11. This contract contains the terms required for a data processing agreement  
218 under UK data protection legislation.
- 219 12. We will help you to comply with your duties under UK data protection  
220 legislation. In most cases you can use the tools we provide. If you ask us  
221 for extra help in complying we will give it to you, but we may charge you  
222 our costs in helping. More detail is provided in Annex A: Tapestry Data  
223 Protection.
- 224 13. If you wish to audit us under UK data protection legislation, you may do  
225 so, but we may charge you our costs in participating in your audit.

## 226 **Our tutorials**

- 227 14. You may copy, store, share and adapt our tutorials for the purpose of  
228 making better use of Tapestry.

## 229 **Our Billing and Support System**

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

## 235 **Our Discussion Forum**

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

## 239 **Fees**

- 240 17. You must pay our fee in full before we will start your Tapestry subscription
- 241 18. Our fee, as set out on our website, is based on the maximum number of  
242 children you wish to have in your Tapestry account during the 12 month  
243 subscription.
- 244 19. You can add or remove individual children throughout the year so long as  
245 the maximum number of children is not exceeded at any one moment.
- 246 20. If you have not paid your fee in full then:
- 247 • we may not provide access to Tapestry.
  - 248 • after 90 days, we will delete the data that you have entered into Tapestry.



- 249 21. If you wish to increase the maximum number of children you can have  
250 in your Tapestry account during the 12 month subscription then we will  
251 charge you the difference between what you have paid and the current fee  
252 for an account with the increased number of children. This will not extend  
253 your subscription.
- 254 22. You must pay us UK Pounds Sterling including any applicable VAT. If  
255 you choose to pay by bank transfer you must bear all currency conversion  
256 and bank transfer costs.

## 257 Termination

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

## 270 Changes and disputes

- 271 25. If something goes wrong, unless otherwise required by law, our total liability  
272 to each other is limited to the annual fee that you have paid us for Tapestry.
- 273 26. One example of where the law requires different liability is in breaches  
274 of UK data protection law. We can both be investigated and fined by  
275 the relevant supervisory authorities and we both may be liable to pay  
276 compensation for damages caused by breaching this law. If it later turns  
277 out that one or other of us wasn't responsible for the breach, then we can  
278 claim back the share of liability from the responsible party.
- 279 27. Our contract with you is under English law and any dispute will be settled  
280 by an English court.
- 281 28. This document, together with its annexes are our entire contract with you.  
282 If you want to vary this contract, or add additional terms, then there will  
283 need to be written and explicit agreement between you and one of our  
284 company directors. To keep our costs and prices down, we rarely do this.  
285 In particular, unless explicitly agreed to by one of our company directors,  
286 we do not accept any standard purchasing terms and conditions that you  
287 may usually apply.
- 288 29. We may change this contract, but will give you reasonable warning.

## 289 **Annex A: Tapestry Data Protection**

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

293 You are a childminder, educator, nursery, school or similar educational organisa-  
294 tion.

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

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

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

### 303 **The legally required terms in a Data Processing Agreement** 304 **or Contract**

305 If you are in the EU, then you must have a written contract with us (sometimes  
306 known as a Data Processing Agreement) and, legally, must include some partic-  
307 ular bits of information and commitments. This contract acts as that written  
308 contract and contains the required information and commitments.

309 To help you find them:

- 310 • The subject matter and duration of the processing is summarised below  
311 under ‘What data is placed into Tapestry’ and set out in detail in Annex  
312 C: Tapestry Privacy
- 313 • The nature and purpose of the processing is summarised below under  
314 ‘What data is placed into Tapestry’ and set out in detail in Annex C:  
315 Tapestry Privacy.
- 316 • The type of personal data and categories of data subject is summarised  
317 below under ‘What data is placed into Tapestry’ and set out in detail in  
318 Annex C: Tapestry Privacy.
- 319 • The obligations and rights of the controller is set out in “What we expect  
320 of you” and “What you can expect of us” below.
- 321 • The standard requirements on data processors (e.g., to act on written  
322 instructions, submit to audit, notify of breaches etc) are set out in “What  
323 you can expect of us” below.

## 324 **Our jurisdiction**

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

326 Our lead supervisory authority for data protection is the UK Information Com-  
327 missioner's Office (<https://ico.org.uk>).

## 328 **Where is data stored?**

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

330 The primary processing and storage location is in Ireland.

331 Our offsite backups are stored in Germany.

332 Our office is in the UK.

333 For the avoidance of doubt: The storage location is part of your contract with us.  
334 If we wished to change where your data is stored, we would need to change this  
335 contract, and contract changes always require agreement from both you and us.

336 To provide a little more detail:

- 337 • Almost all storage and processing is carried out on computers and networks  
338 provided by Amazon Web Services (AWS) a sub-processor who we list in  
339 Annex D. We instruct them to only store data on computers in their data  
340 centres located in Ireland (for the primary system) and Germany (for the  
341 backup system). They are contractually bound not to move data elsewhere  
342 without our permission.
- 343 • The exceptions are:
  - 344 – On very rare occasions, and subject to strict safeguards, we may store  
345 and process some data locally in our offices in order to diagnose or  
346 fix a bug. On these occasions data will be stored and processed in  
347 Lewes in the UK. Some of the safeguards are: we only do it when we  
348 have to – it is never routine; we store the minimum possible amount  
349 of data locally; we only store it on encrypted secure machines; we  
350 delete it as soon as possible.
  - 351 – If you log into Tapestry when you are outside the EU, data will be  
352 transferred outside of the EU to get to you. This is unlikely to be a  
353 concern if you are a non-EU school or nursery because you won't be  
354 storing data about people who are in the EU. It is also unlikely to be  
355 a concern if it only happens every now and again and only concerns a  
356 few children (i.e., a parent does it). However, if you are an EU based  
357 organisation, you should consider your policies for allowing staff to  
358 log into Tapestry if they are outside the EU.

## 359 What data is placed into Tapestry?

360 Annex C: Tapestry Privacy sets out the subject matter and duration of our  
361 processing; the nature and purpose of the processing; the type of personal data  
362 and the categories of data subject.

363 In summary:

- 364 • The categories of data subject are the people you add to Tapestry. Typically  
365 children, staff and relatives of the children. You choose exactly who.
- 366 • The subject matter and types of personal data are typically: names, email  
367 addresses, dates of birth, post codes, contents of an online learning journal,  
368 records of a child's care. You choose exactly what data.
- 369 • The nature and purpose of the processing is typically: to provide an online  
370 record of children's progress and care in order to monitor, share and analyse  
371 that progress and care. You choose exactly what is done with the data  
372 and who it is shared with.
- 373 • The duration of the processing is, at most, the duration of this contract  
374 plus the time taken for data to leave our backup system. It can be shorter  
375 if you choose to delete some or all of your data sooner.

## 376 Who is responsible for what?

377 The first thing to agree is that:

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

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

383 You must:

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

388 We must:

- 389 • Only process data on your instructions.
- 390 • Ensure that people we use to process your data are subject to a duty of  
391 confidence.
- 392 • Take appropriate measures to ensure the security of our processing.
- 393 • Only engage sub-processors with your prior written consent (see Annex  
394 D).
- 395 • Assist you in providing subject access and allowing data subjects to exercise  
396 their rights under data protection law.

- 397 • Assist you in meeting your legal data protection obligations in relation to:
  - 398 – the security of processing.
  - 399 – the notification of personal data breaches.
  - 400 – data protection impact assessments.
- 401 • Delete or return all personal data to you as requested at the end of the
- 402 contract.
- 403 • Submit to your audits and inspections.
- 404 • Provide you with the information to meet your legal obligations.
- 405 • Tell you if we become aware of a data breach
- 406 • Tell you immediately if we are asked to do something infringing data
- 407 protection law.

## 408 **What we expect of you**

### 409 **You must have a lawful basis for putting data into Tapestry**

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

414 Please don't leap to assuming consent is the only lawful basis for you, but  
415 carefully consider the six possible bases described in law and work out which is  
416 right, given what you intend to store in Tapestry and how you intend to use and  
417 share it.

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

### 421 **You must use Tapestry in a way that is compliant with data protection** 422 **law**

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

- 425 1. Processed lawfully, fairly and in a transparent manner in relation to  
426 individuals.
- 427 2. Collected for specified, explicit and legitimate purposes and not further  
428 processed in a manner that is incompatible with those purposes; further  
429 processing for archiving purposes in the public interest, scientific or historical  
430 research purposes or statistical purposes shall not be considered to be  
431 incompatible with the initial purposes.
- 432 3. Adequate, relevant and limited to what is necessary in relation to the  
433 purposes for which they are processed.

- 434 4. Accurate and, where necessary, kept up to date; every reasonable step  
435 must be taken to ensure that personal data that are inaccurate, having  
436 regard to the purposes for which they are processed, are erased or rectified  
437 without delay.
- 438 5. Kept in a form which permits identification of data subjects for no longer  
439 than is necessary for the purposes for which the personal data are processed;  
440 personal data may be stored for longer periods insofar as the personal  
441 data will be processed solely for archiving purposes in the public interest,  
442 scientific or historical research purposes or statistical purposes subject to  
443 implementation of the appropriate technical and organisational measures  
444 required by the GDPR in order to safeguard the rights and freedoms of  
445 individuals.
- 446 6. Processed in a manner that ensures appropriate security of the personal  
447 data, including protection against unauthorised or unlawful processing and  
448 against accidental loss, destruction or damage, using appropriate technical  
449 or organisational measures.

450 Source: [https://ico.org.uk/for-organisations/data-protection-reform/overview-](https://ico.org.uk/for-organisations/data-protection-reform/overview-of-the-gdpr/principles/)  
451 [of-the-gdpr/principles/](https://ico.org.uk/for-organisations/data-protection-reform/overview-of-the-gdpr/principles/)

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

### 453 **You must respond to data protection requests**

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

- 457 1. The right to be informed
- 458 2. The right of access
- 459 3. The right to rectification
- 460 4. The right to erasure
- 461 5. The right to restrict processing
- 462 6. The right to data portability
- 463 7. The right to object
- 464 8. Rights in relation to automated decision making and profiling

465 Source: [https://ico.org.uk/for-organisations/data-protection-reform/overview-](https://ico.org.uk/for-organisations/data-protection-reform/overview-of-the-gdpr/individuals-rights/)  
466 [of-the-gdpr/individuals-rights/](https://ico.org.uk/for-organisations/data-protection-reform/overview-of-the-gdpr/individuals-rights/)

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

### 469 **The right to be informed**

470 In particular, please ensure you proactively dealt with the “right to be informed”  
471 – you must not wait for people to ask you.

472 The UK Information Commissioner’s Office has advice on this: <https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/individual-rights/right-to-be-informed/>.

475 You may wish to use our ‘Annex C: Tapestry Privacy’ as a starting point for  
476 informing your staff and the relatives and children whose data you add to  
477 Tapestry. But you will probably need to adapt it to cover: your contact details,  
478 your lawful basis for adding data, who you intend to share the data with and why  
479 and when you intend to delete the data. Since the new data protection law covers  
480 all data, whether it is on computer or on paper, you may wish to incorporate  
481 this into a single wider document that covers all the data you process.

## 482 **You must keep your contact details on Tapestry up to date**

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

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

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

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

## 495 **What you can expect of us**

### 496 **We will only process data on your written instructions**

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

499 To be absolutely clear: we don’t license or claim ownership of your data; we  
500 don’t sell your data; we don’t use your data for advertising; we don’t pass on  
501 your data except when you instruct us to.

502 You can add users to Tapestry who, depending on the level of access you give  
503 them, can then also instruct Tapestry. You can adjust what data those users see  
504 and what they can do with the data.

505 People whose data you have added to Tapestry have a right to restrict processing.  
506 If you have been told by someone to restrict processing of their data, then

507 you are responsible for not using Tapestry to do any further processing of that  
508 person's data. You are responsible for ensuring any users that you have added to  
509 Tapestry do no further processing. The easiest way to do that is to use Tapestry  
510 to mark the child or user as inactive.

### 511 **Who can instruct us**

512 We prefer to accept instructions through the Tapestry web interface or apps.  
513 This interface has options for authorising different users and giving them different  
514 levels of permission about what they can instruct us to do.

515 We may also accept instructions through our support ticket system or by email  
516 if they come from:

- 517 • Someone who we have verified is registered on the relevant Tapestry account  
518 with the status of a 'manager'.
- 519 • Someone who we have verified is an appropriate representative of the  
520 account owner (e.g., the head of a school, or the director or manager of a  
521 nursery).

522 Depending on the nature of the instruction and the route by which we receive  
523 the instruction, we may need to take extra steps to verify that the instruction is  
524 legitimate. This may lead to a delay in us carrying out the instruction.

525 If someone who isn't authorised tries to instruct us to do something, we will  
526 tell you about it. For example, this most commonly applies to relatives you add  
527 to the Tapestry account who ask us for access to their children's data because  
528 they cannot log in or you haven't provided them with data they think they are  
529 entitled to. We will direct those relatives back to you.

### 530 **What does only 'written' instructions mean?**

531 Under data protection law, we are not allowed to accept verbal instructions for  
532 data processing.

533 If you speak to us face to face or by telephone, you will need you to confirm any  
534 instructions you give us by:

- 535 • Carrying them out yourself through the Tapestry web interface or app
- 536 • Replying to our emailed summary of your instructions, confirming that  
537 you wish us to proceed.
- 538 • Repeating your instructions in a message through our support ticket system,
- 539 • Repeating your instructions by email,
- 540 • Repeating your in a letter to us.

### 541 **Instructions we do and don't accept**



542 Sometimes our customers write to us with a ‘data processing agreement’ or ‘data  
543 processing schedule’ that sets out how they intend to use Tapestry (e.g., they  
544 intend to use Tapestry to store assessments, but not pictures and videos and  
545 intend to share those with other staff but not relatives). It is important to note  
546 that while we don’t require you to store any particular data about any particular  
547 person, we also don’t prevent you from storing any particular data about any  
548 particular person. So, in the case of the example, if an authorised member of  
549 staff later chose to upload a video or share an observation with a relative, we  
550 would not stop them.

551 What this means is that we cannot limit your use of Tapestry beyond the options  
552 we give users with ‘manager’ accounts on Tapestry to set permissions for other  
553 users. If you instruct us to apply further limitations, for example by sending  
554 us a schedule describing how you intend to use Tapestry, we cannot comply.  
555 However, we are always happy to provide you with help and guidance in how to  
556 set permissions within Tapestry to meet your needs.

557 Similarly, whilst we are always keen to receive suggestions about how to improve  
558 our security, we cannot accept instructions to apply particular security measures  
559 to your account that aren’t already available in the Tapestry control panel. For  
560 example, we cannot currently accept instructions to restrict access to Tapestry  
561 for particular users to particular locations or times of day, though we have got  
562 features like that on our todo list.

### 563 **We will ensure that people we use to process your data are subject** 564 **to a duty of confidence**

565 Our staff who process your data are:

- 566 1. Contractually bound to keep your data confidential.
- 567 2. Vetted by us. This includes a DBS check, which is updated annually.
- 568 3. Appropriately trained in data protection.

### 569 **We will take appropriate measures to ensure the security of our pro-** 570 **cessing**

571 The measures we take are described in Annex B.

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

### 574 **We will engage sub-processors only with your prior consent**

575 We use sub-processors in a way that is compliant with UK data protection law.  
576 Our sub-processors, what they do, and our process for seeking your agreement  
577 to any changes are described in Annex D.

578 **We will assist you in providing subject access and allowing data sub-**  
579 **jects to exercise their rights under data protection law**

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

581 We provide a section in the control panel where you can download a single file  
582 that brings together all the information Tapestry holds about a particular child  
583 or a particular user.

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

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

586 **We will assist you in meeting your legal data protection obligations**

587 **The security of processing**

588 We describe our current security approach in Annex B.

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

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

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

596 **Notification of personal data breaches**

597 If we become aware of, or suspect, a data breach, we will tell you without undue  
598 delay. If you become aware of, or suspect, a breach, please tell us as soon as you  
599 can.

600 If there is a personal data breach, we will:

- 601 1. Help you to prevent further breaches (e.g., if someone has stolen a computer  
602 used by you to log into Tapestry, and you are concerned that your Tapestry  
603 password was stored on that computer, we can disable the relevant accounts  
604 and change the relevant passwords).
- 605 2. Help you to work out who has been affected.
- 606 3. Help you to work out what data may have been breached.
- 607 4. Help you to determine the cause of the breach.
- 608 5. Help you in your dealing with the Information Commissioners Office.

609 The Information Commissioners Office require you to notify them of any data  
610 breach that is “likely to result in a risk to the rights and freedoms of individuals”  
611 within 72 hours of you becoming aware of it. We will prioritise our work to help  
612 you to meet that deadline.

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

#### 615 **Data protection impact assessments**

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

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

#### 620 **We will delete or return all personal data to you as requested at the** 621 **end of the contract**

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

623 At the end of the contract our standard practice is to delete your data from  
624 our systems after 90 days. The data will be deleted from our backup systems  
625 90 days after it is deleted from our systems. We are happy to delete your data  
626 sooner if you ask us to.

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

630 We will not delete data if we are required by law to keep it (for instance, for an  
631 ongoing police or data protection investigation).

#### 632 **We will submit to your audits and inspections**

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

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

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

#### 639 **We will provide you with the information to meet your legal obliga-** 640 **tions**

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

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

#### 646 **We will tell you if we become aware of a data breach**

647 If we become aware of a data breach, we will tell you about it and help you to  
648 meet your obligations as we've described above. We will do this without undue  
649 delay. Please keep your contact details up to date so that we can contact you  
650 quickly.

651 If we suspect a possible data breach we may 'lock down' access to Tapestry if  
652 we think that would help prevent a further breach. This would mean that some  
653 or all users of Tapestry would lose partial or complete access to Tapestry while  
654 we investigate and fix whatever led to the breach. We would inform you as soon  
655 as possible if we need to do this.

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

658 If we are asked to do something that we believe infringes data protection law we  
659 will not do so, and we will try and reach you through the contact details you  
660 have given us to explain what has happened.

### 661 **If something goes wrong**

#### 662 **Complaints**

663 If you have a complaint, then please contact us at [customer.service@eyfs.info](mailto:customer.service@eyfs.info).

#### 664 **Our Data Protection Officer**

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

667 Lauren Foley [dpo@eyfs.info](mailto:dpo@eyfs.info) 1 Southdown Avenue Lewes BN7 1EL UK

668 **Frequently Asked Questions**

669 **With regard to Brexit: will the data be hosted and backed**  
670 **up in the UK once Brexit is finalised?**

671 We do not know yet how data protection law will change with Brexit. But we  
672 are keeping an eye on developments and will make whatever changes are required  
673 to be compliant with UK data protection law as it changes.

## 674 **Annex B: Tapestry Security**

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

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

### 683 **Security Responsibilities**

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

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

### 690 **Who are we?**

691 Tapestry is the name of a product that was conceived, developed and is owned by  
692 The Foundation Stage Forum Ltd., an early years organisation that has provided  
693 resources and support for the early years workforce since February 2003. We  
694 have contracts with many local authorities, some of which have been in place for  
695 ten or more years.

### 696 **The Foundation Stage Forum Ltd**

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

699 Our company number is 05757213.

700 Our registered office is at:

701 1, Southdown Avenue  
702 Lewes  
703 East Sussex  
704 BN7 1EL

705 Our VAT registration number is 932933317.

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

708 Our contracts are under UK law.

709 We have two directors: Helen and Stephen Edwards.

#### 710 **Director: Stephen Edwards MSc**

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

718 Steve is the board member responsible for security.

#### 719 **Director: Helen Edwards DPhil**

720 Helen has been working with young children since 1989, firstly as a primary  
721 school teacher, and then as a successful nursery owner/manager, followed by  
722 employment as a local authority advisor and university tutor, and more recently  
723 as an Ofsted inspector. She also holds the EYP status.

#### 724 **Data Protection Officer: Lauren Foley**

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

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

#### 729 **Data Protection Law**

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

732 To summarise it in brief: You, the Tapestry account manager, own the data you  
733 put on Tapestry. We, Foundation Stage Forum Ltd, do not. In technical terms,  
734 you are the Data Controller, we are the Data Processor.

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

737 We will not access your data without your permission.

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

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

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

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

## 750 Access to data

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

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

756 We will not give Tapestry account information, or access to your Tapestry account,  
757 to anyone other than those individuals you have set up as staff members.

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

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

## 765 Deleting data when it is no longer needed

766 You can modify and delete the data you enter.

767 In the common case of children leaving your setting, you can move them into a  
768 'deleted' area, where (after a delay of ninety days to avoid disastrous mistakes



769 occurring) their data will be deleted (this includes relevant pictures, videos,  
770 journals and reports).

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

774 If you let your subscription to Tapestry lapse, we will delete all data associated  
775 with it. We delay the deletion for 90 days in case your subscription has inadver-  
776 tently lapsed (e.g., it happened while you are on holiday, or there was a delay in  
777 your Local Authority paying our invoice) but if you explicitly ask us to then we  
778 will delete your data immediately.

779 Data will remain in our backups for 90 further days. If you wish, you can instruct  
780 us to to delete *all* your data from these backups. But it is all or nothing. We  
781 cannot delete *some* of your data on these backups.

782 Once the data is deleted from our backups we can no longer recover it.

## 783 **Organisational data security**

### 784 **ISO 27001**

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

788 Our data centre, Amazon Web Services, has been independently certified as ISO  
789 27001 compliant.

### 790 **Staff**

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

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

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

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

## 802 **Procedures**

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

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

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

812 For instance, you should think about:

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

## 821 **Passwords**

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

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

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

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

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

838 You can choose a minimum password strength that you permit the people you  
839 add to Tapestry to use. We won't let this minimum be any less than 10 characters  
840 and we allow and encourage you to set a tougher standard than that (by, for  
841 instance, requiring longer passwords).

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

845 If you wish, you can set an initial password and PIN for the staff and relatives  
846 that you add, but we strongly discourage this. We prefer you to use the option  
847 of sending links that allow users to set their own passwords and PIN without  
848 you seeing them.

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

853 If you have lost access to your email address associated with Tapestry, or you  
854 have taken over a Tapestry account due to the departure of the previous account  
855 owner and don't have access, then we can add an email address for the new  
856 manager. In order to verify that the request is legitimate we have to take several  
857 steps. Even if these steps are successful, they may mean a delay of weeks during  
858 which time Tapestry may not be accessible by you. To avoid this, please ensure  
859 you update contact details before a manager departs and, ideally, always register  
860 more than one manager on the Tapestry system.

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

864 If you believe the password for one or more accounts has or could have been  
865 compromised, please immediately make that account inactive using the Tapestry  
866 control panel or, if you are unable to do so, contact us and we will do it for you.  
867 Please then contact us to discuss how to re-activate the accounts in a way that  
868 ensures they remain secure.

869 Because passwords can be reset by email, if you believe that the email account  
870 associated with a Tapestry account has been compromised, please treat it as if  
871 the password has been compromised: make the Tapestry account inactive and  
872 contact us.

## 873 **Technical data security**

874 The Tapestry web service and data are hosted in a cloud hosting environment  
875 operated by AWS in the EU (primarily the Republic of Ireland, with backups in

876 Germany). AWS is the largest cloud hosting provider in the world and provides  
877 a secure platform for some of the world's largest online service providers.

## 878 **Physical security**

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

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

891 We make sure that the devices we use to connect to the Tapestry servers are  
892 physically secure.

893 We also don't routinely store any of your data on our local devices. It is usually  
894 only stored on our servers. On the very rare occasions when we have to (in order,  
895 for instance, to diagnose a bug which we have not been able to replicate in any  
896 other way), we store as little as possible, for as short as time as possible, with  
897 access limited to as few people as possible. We also ensure that the machines we  
898 store it on are secure, including ensuring that their storage is encrypted.

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

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

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

913 The iOS and Android Tapestry apps don't store passwords locally, only tem-  
914 porarily store some data (such as copies of images that are being shown on

915 screen), and require a password or pin to be entered to open the app. Therefore,  
916 if the device is stolen, the person who stole it would not have significant access  
917 to Tapestry data without guessing your password or PIN.

918 The devices may have copies of the pictures and videos that have been taken  
919 outside of the app. There is also a setting that allows copies of pictures and  
920 videos taken within the app to be stored in the device's picture gallery. However,  
921 by default this setting is disabled. If you download data (such as PDFs of  
922 journals) from Tapestry to your device, those are at risk.

### 923 **Software security**

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

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

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

### 932 **Encryption**

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

938 Connections between the Tapestry apps and our servers are similarly encrypted.

939 Connections between our office computers and Tapestry are encrypted.

940 Your data is encrypted at rest on our servers. This includes our backups of your  
941 data.

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

949 The SHA1 fingerprint of our certificate is DC F6 23 A3 35 97 98 98 6E 6B 29 91  
950 51 B2 35 93 DA 1F 7F DC

**951 Partitioning**

952 Our network is partitioned to provide minimum access between our servers and  
953 the internet. In particular, our databases cannot directly access or be accessed  
954 from the internet, but only from specific servers. Only a handful of servers  
955 can be accessed from the internet, and only on specific ports and using specific  
956 protocols (e.g., no unencrypted connections are permitted). This reduces the  
957 likelihood that external hackers can gain access to our servers and then get data  
958 out.

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

963 Our software is partitioned so that it only has the minimum level of privileges  
964 to carry out whatever task it is currently doing. This reduces the likelihood  
965 that somebody who hacked into one part of our code could use it to compromise  
966 other areas.

**967 Logging**

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

**971 Verification (also known as Penetration Testing)**

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

975 The penetration tests cover both the web and the app versions of Tapestry.

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

979 The most recent check was in August 2017. If you have a legitimate interest in  
980 Tapestry (e.g., you are the account owner or a parent) we are happy to summarise  
981 what they found.

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

## 984 **Capacity, Redundancy and Backups**

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

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

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

994 We also retain backups of all data in a different physical location (at the time  
995 of writing, the primary physical locations are in the Republic of Ireland, the  
996 backup physical locations are in Germany).

997 These backups should be, at most, 24 hours old and we should have 90 days of  
998 backups.

999 The backups are treated with the same care as the primary data (in particular,  
1000 they are encrypted in transit and rest and stored in AWS facilities with the same  
1001 physical security as described in the 'physical security' section above).

1002 Please note that backups are for disaster recovery. We will use them to restore  
1003 your data should it become lost or corrupted on the live system. It is not designed  
1004 for easy access to restore specific bits of data that you have deliberately deleted  
1005 from the live system. If you ask us to retrieve specific bits of information from  
1006 the backups, we will do so, but we may need to charge our costs.

## 1007 **Keeping in touch about security**

1008 If you suspect a security issue (e.g., you believe that passwords on your account  
1009 may be compromised because, for instance, computers have been stolen) then  
1010 email us at [customer.service@eyfs.info](mailto:customer.service@eyfs.info). Please include a descriptive subject line  
1011 in your email (i.e., don't just say "Help!" but say "Help! Our computers have  
1012 been stolen").

1013 If we have a security concern about your account, we will try and reach the  
1014 primary contact we have listed. This will initially be the person that set up the  
1015 account. You can change this using the Control Panel within Tapestry (Settings  
1016 > Contact Details). Please keep this information up to date.

1017 If you or we suspect a security problem, our first step will usually be to lock  
1018 down the accounts whilst we work together to establish what happened and the  
1019 best course of action.

**1020 Frequently asked security questions**

1021 Below are some frequently asked questions that relate to security. If you have a  
1022 question that hasn't been covered by this document, please ask us at customer.  
1023 service@eyfs.info. Please note that, for security reasons, we may not answer  
1024 some questions (such as, for instance, the exact versions of software that we are  
1025 using).

**1026 Can you fill out this security questionnaire for me?**

1027 To keep our price down, we do not enter into bespoke contracts or fill out security  
1028 checklists. However, we hope that our contract, including its annexes, include  
1029 all the answers you need and cover all the events that you are concerned about  
1030 and that you can use them to fill out whatever paperwork you require for your  
1031 own systems.

1032 If you have questions about our service that aren't covered then do get in touch  
1033 and, if we can, we will add the answers to this contract.

**1034 Do you offer a service level agreement?**

1035 To keep our price down, we do not. However, we take fulfilling our obligations to  
1036 you very seriously and will do our utmost to ensure our service is there whenever  
1037 you need it.

**1038 Are you insured?**

1039 Yes. Our insurance covers the standard corporate liabilities. In addition, it  
1040 covers liabilities relating to hacking and relating to data breaches. Like all  
1041 insurance it is subject to excesses, limits and exclusions.

**1042 What happens if my account subscription should expire?**

1043 We want to avoid painful mistakes happening because, for instance, a subscription  
1044 expires during a school holiday and nobody is around to pay the bill. So we  
1045 do not immediately delete your data when your subscription expires unless you  
1046 specifically ask us to.

1047 However, 90 days after your subscription expires we will permanently delete your  
1048 data. Data will remain in our backups for 90 further days.

1049 If you wish, you can instruct us to delete all your data sooner.



1050 **Do you store data outside of the EU?**

1051 No.

1052 **What encryption principles are used for data in transit?**

1053 We regularly check our encryption meets modern standards and improve it as  
1054 appropriate. At the moment we use a 2048 bit key, SHA256 with RSA and allow  
1055 TLS1.0, TLS1.1, and TLS1.2.

1056 **Have you disabled TLS 1.0 support?**

1057 Not yet: An appreciable proportion of our customers still use devices that are  
1058 only able to use TLS 1.0.

1059 However, we are keeping this under regular review and would strongly like to  
1060 disable it at some point this year.

1061 **What encryption key management processes are in place?**

1062 We use AWS to manage our encryption keys and provide them to authorised  
1063 servers at the right moment.

1064 **The data centre hosting Tapestry is ISO 27001 accredited. Which  
1065 version of ISO 27001 is it, and who is the accrediting company?**

1066 The version is 2013, and the accrediting company is BMTRADA.

1067 **Do you follow any other standards or hold any other certifications?**

1068 Unless mentioned above, no. We take security very seriously and regularly  
1069 review what we do. But we have not yet, for instance, undergone ISO27001  
1070 accreditation as a business.

1071 **Which board member is responsible for security?**

1072 Our Managing Director, Stephen Edwards, is responsible for security.

1073 **Do you have a documented framework for security governance, with**  
1074 **policies governing key aspects of information security relevant to the**  
1075 **service?**

1076 We do not yet have a complete set of documentation. We have started on the  
1077 process of creating an ISO 27001 compliant documentation set, but the process  
1078 is not yet complete.

1079 **Can you provide evidence that security and information security are**  
1080 **part of your financial and operational risk reporting mechanisms, en-**  
1081 **suring that the board would be kept informed of security and infor-**  
1082 **mation risk?**

1083 We are a small firm so our board, Stephen Edwards and Helen Edwards, are  
1084 closely involved in every decision taken by the firm.

1085 We are very aware of the importance of information security. We discuss it in  
1086 almost every meeting and we continuously attempt to improve our security.

1087 We have a weekly formal review of our security state (see above)

1088 We get independent penetration testers to review our system (see above)

1089 **Can you provide evidence of processes to identify and ensure compli-**  
1090 **ance with applicable legal and regulatory requirements?**

1091 We discuss compliance in almost every meeting, particularly during this period  
1092 of transition to the GDPR.

1093 We have appointed a Data Protection Officer to hold us to account on this point.

1094 **Do you track the status, location and configuration of service com-**  
1095 **ponents throughout their lifetime?**

1096 Yes. Our software configuration is managed under version control, with repeatable  
1097 builds and change logging.

1098 Yes. Our hardware configuration is managed under version control, with repeat-  
1099 able builds and change logging.

1100 **Do you assess changes to the service for potential security impact and**  
1101 **monitor that impact to completion?**

1102 Yes.

1103 **How are potential new threats, vulnerabilities or exploitation tech-**  
1104 **niques which could affect the service assessed?**

1105 We run regular automated tests and internal security reviews to examine the  
1106 configuration and security of our servers.

1107 We engage external penetration testers to assess our system against the latest  
1108 threats.

1109 **Do we use relevant sources of information relating to threat, vulner-**  
1110 **ability and exploitation techniques, eg NIST, NCSC?**

1111 Yes. We monitor CVEs relating to the software our service depends on.

1112 Yes. We regularly review guidance from the NCSC and OSWAP. We do not  
1113 regularly review guidance from NIST.

1114 **How are known vulnerabilities prioritised and tracked until mitiga-**  
1115 **tions have been deployed?**

1116 We have automated notifications of vulnerabilities that are in our deployed code.  
1117 These notifications are only quietened when fixes have been deployed.

1118 We have internal issue tracking for required code and deployment changes.

1119 We review and prioritise remaining security actions at least once a week.

1120 **What are the timescales for implementing mitigations? E.g. in patch-**  
1121 **ing policy?**

1122 This depends on the vulnerability.

1123 For instance, if we believe the vulnerability could lead to data exposure, we  
1124 would immediately take Tapestry offline while we fix the vulnerability. Because  
1125 Tapestry would be offline, it would be our highest priority to fix. We have  
1126 procedures for calling in engineers out of hours and at weekends. We have  
1127 procedures for deploying changes to our production configuration within hours.

1128 If the vulnerability was assessed as being of low risk, it would be deployed as  
1129 part of our regular code and configuration updates. These tend to be made at  
1130 least once every two weeks and are often made several times a week.

1131 **Other than for fault-finding, are activity logs monitored for suspicious**  
1132 **activity, potential compromises or inappropriate use of the service?**

1133 Activity logs for our backend system have automated alerting for suspicious  
1134 activity. These alerts are seen by all developers and by Stephen Edwards.

1135 Activity logs for our customers are not monitored by us. They are available to  
1136 customers to monitor.

1137 **Do we have an incident management process?**

1138 Yes. An incident will be uniquely identified and a named individual will be  
1139 allocated responsibility for managing an incident through our support system.  
1140 We have standard procedures for common incidents.

1141 **What is the process for the vendor to report incidents to the cus-**  
1142 **tomers?**

1143 See “Keeping in touch about security” above.

1144 **Is 2-factor authentication (2FA) available to end users?**

1145 No. But if sufficient numbers of users ask for it, we will implement it: Get in  
1146 touch with us at [customer.service@eyfs.info](mailto:customer.service@eyfs.info).

1147 **Can we require passwords to be changed every X days?**

1148 No. The UK National Cyber Security Centre recommend that you DO NOT  
1149 require users to change passwords every X days.

1150 If you suspect a password or email account may have been compromised, you can  
1151 make the account inactive and then manually force the password to be changed.  
1152 We can do this in bulk for all accounts if you contact us.

1153 **Which NSCC system architecture do you use?**

1154 Of the list at [https://www.ncsc.gov.uk/guidance/systems-administration-](https://www.ncsc.gov.uk/guidance/systems-administration-architectures)  
1155 [architectures](https://www.ncsc.gov.uk/guidance/systems-administration-architectures) our system is closest to the ‘bastion’ model.

1156 The service is run on partitioned and private networks. Management functions  
1157 are carried out by devices on the corporate network which access the private  
1158 networks through bastions.

1159 **What provision is made for customers to access / monitor audit**  
1160 **records for system / data access?**

1161 Customers have direct self-service access to logs that show changes to data.

1162 We can provide logs of who has viewed data on request to customer.service@  
1163 eyfs.info.

1164 **Does your organisation have differentiated access to data depending**  
1165 **on the sensitivity level?**

1166 Yes. Our default is ‘no access’ and our systems are designed to minimise access  
1167 to data. Different people and the different roles they carry out have different  
1168 access to data and different requirements for what authorisation they must have  
1169 before accessing it. We regularly review who can access what and why to ensure  
1170 we are private and secure by default.

## 1171 **Annex C: Tapestry Privacy**

1172 This annex describes our privacy policy for people who access the Tapestry  
1173 online learning journal service, (<https://tapestryjournal.com>). This policy is  
1174 intended to be shared with any person who uses Tapestry as part of their  
1175 “right to be informed” under UK data protection law. Since we operate as  
1176 a Data Processor for our customers, the Data Controller (the childminder,  
1177 educator, nursery, school or similar educational organisation), will need to  
1178 provide extra information to fulfil the “right to be informed”. We describe  
1179 this extra information briefly in ‘Annex A: Tapestry Data Protection’ and  
1180 you can get more guidance from the UK Information Commissioner’s Of-  
1181 fice: [https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-  
1182 regulation-gdpr/individual-rights/right-to-be-informed/](https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/individual-rights/right-to-be-informed/).

1183 We are the Foundation Stage Forum Ltd, a company registered in England with  
1184 company number 05757213 and a registered address of 1, Southdown Avenue,  
1185 Lewes BN7 1EL, UK.

1186 Our customers are childminders, educators, nurseries, schools or similar educa-  
1187 tional organisations.

1188 You are someone who has been given access to Tapestry by one of our customers.  
1189 For example, you could be a member of staff, a relative of a child, the child  
1190 themselves, or someone acting on behalf of a child.

1191 You may have rights under EU Data Protection legislation relating to information  
1192 we store about you. These rights are described here: [https://ico.org.uk/for-the-  
1193 public/](https://ico.org.uk/for-the-public/). If you want to exercise those rights, please contact the customer who  
1194 is storing data in Tapestry in the first instance (e.g., the school or nursery). If  
1195 they want help in carrying out your request, they can contact us.

1196 Our lead supervisory authority for data protection is the UK Information Com-  
1197 missioner’s Office (<https://ico.org.uk>).

### 1198 **The Service**

1199 Our customers pay us to provide them with a service that allows them to create  
1200 online learning journals for children under their care, monitor those children’s  
1201 progress and share this information with their staff and, if they wish, those  
1202 children’s parents and relatives.

### 1203 **What data do we collect?**

1204 Our customers may choose to store some of the following data on our service:

- 1205 • The names and email addresses of their staff

- 1206 • The names, dates of birth and postcode of their children
- 1207 • The names and email addresses of the parents and relatives of their children
- 1208 • The contents of a learning journal:
  - 1209 – assessments of children’s performance
  - 1210 – notes, photographs and videos of the children
- 1211 • A record of the child’s care:
  - 1212 – what they ate and drank
  - 1213 – toileting
  - 1214 – how they slept
  - 1215 – whether they had any accidents

1216 Our customers store this information in order to record, analyse and, if they  
1217 wish, share the progress of their children.

1218 Our customers have the freedom to choose what data they store and who they  
1219 store it about.

1220 Our customers choose who has access to the data.

1221 Our customers are able to correct and delete data at will.

1222 Our customers must tell you, as part of your right to be informed, what data  
1223 they are storing, why they are storing it and who they are sharing it with.

1224 In providing the service, we will send automated emails to staff and parents  
1225 in order to confirm email addresses, reset passwords and notify them of events  
1226 relating to the customer (such as when a new observation is added about a child).  
1227 We never send any marketing information, though we do send staff a newsletter  
1228 about Tapestry.

1229 We ONLY access the data stored by our customers in order to carry out our  
1230 customer’s instructions, to maintain or improve the service or to fix faults.  
1231 We do not use our customer’s data for marketing. We use sub-contractors to  
1232 process some of the data, but we do not otherwise share this data with other  
1233 organisations.

1234 If your contact details are registered on Tapestry in the ‘contact details’ section,  
1235 or as a ‘manager’ then we may contact you if we have a question or concern  
1236 about the associated Tapestry account.

1237 When you visit the Tapestry web site we collect your:

- 1238 • IP address, together with
- 1239 • Information your computer sends about its web browser and operating  
1240 system, and
- 1241 • What pages you look at (e.g., the list of observations), but not the content  
1242 of those pages (i.e., we could not tell directly from the data whether the  
1243 list of observations contained information about a particular child, though  
1244 given time and access to the data above it would be possible to figure that  
1245 out).

1246 We use this information to monitor the security of our service, to help us figure  
1247 out how to improve the service (e.g., what browsers should we support? How  
1248 much capacity should we add?) and to improve the way we market the service  
1249 (e.g., what search terms were used to discover our site). We do not share it.

1250 If you use our phone or tablet application we collect:

- 1251 • The IP address of the network your phone or tablet is on, together with
- 1252 • The make and model of your phone or tablet, together with
- 1253 • The version of your phone or tablet’s operating system, together with
- 1254 • Details of any crashes that occur in the application, and
- 1255 • What screens you look at in the application (e.g., the list of observations),  
1256 but not the content of those screens (i.e., we could not tell directly from  
1257 the data whether the list of observations contained information about a  
1258 particular child, though given time and access to the data above it would  
1259 be possible to figure that out).

1260 We use this information to monitor the security of our service and to help us  
1261 figure out how to improve the service (e.g., what causes crashes? which crashes  
1262 need fixing most urgently?). We do not share it.

## 1263 **What is the lawful basis for storing this data**

1264 Our customers decide and must tell you the lawful basis for the data they add  
1265 to Tapestry. Please note, your consent is not the only lawful basis for storing  
1266 data and our customers may have a different legal basis.

## 1267 **Whose data is it?**

1268 We don’t claim ownership of the data entered into Tapestry. We only use it  
1269 according to our customer’s instructions to provide the service described above.

1270 Formally, in UK data protection legislation terms, our customers are the “Data  
1271 Controller” and we are the “Data Processor”.

1272 There are three exceptions to this, where we are the “Data Controller”:

- 1273 1. The content of our billing system
- 1274 2. The content of our support ticket system
- 1275 3. The content of our forums

1276 These exceptions are described in more detail in Annex E and Annex F.

## 1277 **Who do we share data with?**

1278 We do not share data, except as explicitly requested by our customers.



1279 If they wished, our customers might give other people (e.g., staff or parents)  
1280 access to data. They might download or print some or all of the data and share  
1281 it with other people (e.g., staff, parents, the government). They might transfer  
1282 some of the data to another organisation (e.g., parents, the government, another  
1283 educational establishment looking after a child).

1284 We ONLY access the data stored by our customers in order to carry out our  
1285 customer's instructions, to maintain or improve the service, or to fix faults.

### 1286 **How do we collect the data?**

1287 Most data is entered by our customers directly into our website or through our  
1288 phone and tablet applications. Our customers may, if they wish, permit parents  
1289 and relatives of children to add data to the service.

1290 Some data (described above) is sent automatically by your web browser or by  
1291 our applications.

1292 We may store cookies on your computer in order to verify that you are logged  
1293 in and to store your preferences. The cookies themselves do not contain any  
1294 identifiable information about you or about what you look at.

### 1295 **Can I see my data that is stored on your system?**

1296 Yes. The school, childminder, nursery or similar educational organisation, can  
1297 give you a copy of data about you that they or you have stored in Tapestry. We  
1298 can provide you with a copy of any of the other data that has been collected  
1299 (e.g., our records of your IP address and / or make and model of your tablets  
1300 etc.).

### 1301 **Can I have my data corrected or deleted?**

1302 Yes. The school, childminder, nursery or similar educational organisation, can  
1303 correct or delete the data they or you have stored in Tapestry.

1304 The process of deletion is gradual: initially deleted data is moved to a 'deleted'  
1305 area in case it was deleted in error. After a delay, it is then permanently deleted  
1306 from our main systems. After a further delay, it is then permanently deleted  
1307 from our backups.

### 1308 **What are our customer's responsibilities?**

1309 Our customers decide who to add data about, what data to add, and how long to  
1310 keep it for. They have overall responsibility for complying with Data Protection

1311 law (or the equivalent in other countries).

1312 We describe this in more detail in the contract we have with our customers. But,  
1313 for instance, they have to:

- 1314 • Ensure they have a legal basis for what data they store on Tapestry and  
1315 who they share it with.
- 1316 • Think about what information it is appropriate to share with whom, given  
1317 their situation and that of the children under their care.
- 1318 • Respond to requests for access to data.
- 1319 • Train their staff about sensible security and confidentiality precautions:
  - 1320 – Taking care of passwords.
  - 1321 – Taking care not to install software on computers that may compromise  
1322 security.
  - 1323 – Taking care not to access material from inappropriate places where it  
1324 can't be kept appropriately confidential.
- 1325 • Delete data when it is no longer required.
- 1326 • Remove access for people who no longer need access.
- 1327 • Give parents instructions in accordance with their safeguarding policy.

## 1328 **Contacting Us**

1329 You can contact us at [customer.service@eyfs.info](mailto:customer.service@eyfs.info) or 1, Southdown Avenue, Lewes  
1330 BN7 1EL, UK.

1331 We also have a Data Protection Officer, Lauren Foley, who can be reached at  
1332 [dpo@eyfs.info](mailto:dpo@eyfs.info).

1333 **Annex D: Tapestry Sub-processors**

1334 Not all parts of Tapestry are run in-house. Below are a list of the sub-contractors  
1335 that we use to process some of your data. They are under a written contract  
1336 that ensures they are compliant with UK data protection law.

1337 For the avoidance of doubt: We are accountable to you for this contract. If one  
1338 of our sub-processors does something wrong, it is our fault – we won't pass the  
1339 buck.

1340 For the avoidance of doubt: We instruct our sub-processors in ways that are  
1341 consistent with this contract.

1342 For instance: Although Amazon Web Services have data centres outside of the  
1343 EU and, technically, could move your data there, they are contractually bound  
1344 not to do so without our instruction and we would not instruct them to do so.

1345 For instance: Although Amazon Web Services could, technically, access your  
1346 data, they are contractually bound not to except if it is strictly necessary to  
1347 deliver their service to us. Even then, their employees are contractually obliged  
1348 to keep data confidential and secure.

1349 **List of sub-processors**

1350 To continue to use Tapestry, we require your consent to our use of the following  
1351 sub-processors:

- 1352 • Amazon Web Services. They host Tapestry. They are ISO 27001 compliant.  
1353 Their address is 410 Terry Avenue North Seattle WA 98109-5210.

1354 **Changes to sub-processors**

1355 We may, occasionally, need to add or change the sub-contractors we use to  
1356 process some of your data.

1357 If we do, then UK data protection law requires us to tell you and to obtain your  
1358 agreement.

1359 We've included the list of sub-processors as part of this contract which means  
1360 that if we want to change them we will do so by proposing a change to this  
1361 contract with you. We will give you as much notice as possible so you can discuss  
1362 any changes with us. We will then ask for your written agreement to the change  
1363 in contract.

## 1364 **Annex E: Billing and support data**

- 1365 1. We are the Foundation Stage Forum Ltd, a company registered in England  
1366 with company number 05757213 and a registered address of 1, Southdown  
1367 Avenue, Lewes BN7 1EL, UK.
- 1368 2. You are a childminder, educator, nursery, school or similar educational  
1369 organisation.
- 1370 3. This annex relates to data in our billing and support system. It does not  
1371 relate to data placed in the Tapestry online learning journal (see Annex  
1372 A) or to data placed in our discussion forums (see Annex F).

### 1373 **What data do we collect?**

- 1374 3. We collect the following information about people who contact us by email  
1375 or through our support ticket system:
  - 1376 • The person's email address and the contents of the email
- 1377 4. If you contact us by telephone, post or face-to-face we may also keep notes  
1378 of those interactions.
- 1379 5. We store:
  - 1380 • Your name, email address, telephone number and postal address
  - 1381 • The name, email address and telephone numbers of anyone you tell us who  
1382 administers or pays for your account with us.
- 1383 6. Credit card payment information is given directly to a payment service  
1384 provider. We do not hold any credit card information ourselves.

### 1385 **Why do you need this data?**

- 1386 7. Our lawful basis for collecting this data is 'contract'. We need this data to:
  - 1387 • Charge you for our service.
  - 1388 • Respond to questions or problems raised by you about our service.
  - 1389 • Contact you if we have questions about your account.
  - 1390 • Decide what changes to make to our service.

### 1391 **Who do you share this data with?**

- 1392 8. We make use of subcontractors to provide our service to you and they may  
1393 see some or all of this data:
  - 1394 • Amazon Web Services - For hosting.

- 1395 • Barnian Media Ltd - For technical support.
  - 1396 • SagePay - For managing credit card payments.
  - 1397 • Fastmail - For managing our email
- 1398 10. If you contact us in relation to a particular Tapestry account then we may  
1399 share that data with other people who we believe represent the organisation  
1400 that owns that account. For example, if a teacher contacted us to instruct  
1401 us to permanently delete a particular child's data, and then the head of the  
1402 school later contacted us to ask why a child had been deleted, we would  
1403 share the instruction from the teacher with the head.
- 1404 11. We do not use or share your data for any reason other than to provide or  
1405 improve our service. For the avoidance of doubt: we do not sell your data.

#### 1406 **Where is the data stored?**

- 1407 10. Your data is stored within the EU. Our processing is carried out within  
1408 the EU.

#### 1409 **How long do you keep this data?**

- 1410 11. We keep your data for up to 7 years. We keep data this long in case it is  
1411 required in an audit and to help us decide what changes to make to our  
1412 service.

#### 1413 **How do I exercise my rights under data protection law?**

- 1414 12. We are the data controller of this data.
- 1415 13. Your rights under data protection law are described at [https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-](https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/individual-rights/)  
1416 [regulation-gdpr/individual-rights/](https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/individual-rights/). They include the right to see and  
1417 correct this data.  
1418
- 1419 14. To exercise those rights, contact us at [customer.service@eyfs.info](mailto:customer.service@eyfs.info).
- 1420 15. We also have a Data Protection Officer, Lauren Foley, who can be reached  
1421 at [dpo@eyfs.info](mailto:dpo@eyfs.info).
- 1422 16. Our lead supervisory authority for data protection is the UK Information  
1423 Commissioner's Office (<https://ico.org.uk>).

## 1424 **Annex F: Use of our discussion forum**

- 1425 1. We are the Foundation Stage Forum Ltd, a company registered in England  
1426 with company number 05757213 and a registered address of 1, Southdown  
1427 Avenue, Lewes BN7 1EL, UK.
- 1428 2. You are a childminder, educator, nursery, school or similar educational  
1429 organisation.
- 1430 3. We have a discussion forum (<https://eyfs.info>) that you may use to dis-  
1431 cuss issues facing childminders, educators, nurseries, schools or similar  
1432 educational organisations.

## 1433 **Liability**

- 1434 4. We do not vouch for the accuracy, completeness or usefulness of any  
1435 material on the forum. Use it at your own risk.
- 1436 5. The material expresses the views of the author of the material, and not  
1437 necessarily our views.
- 1438 6. If you feel any material on the forum is objectionable, please contact us  
1439 immediately at [customer.service@eyfs.info](mailto:customer.service@eyfs.info).

## 1440 **Content and ownership of your messages**

- 1441 6. Don't post anything we won't like.
  - 1442 • We like professional discussion of the issues facing childminders, edu-  
1443 cators, nurseries, schools or similar educational organisations.
  - 1444 • We don't like things that are unkind, illegal, lies, use language you  
1445 wouldn't want children to hear, or are shameless advertising.
- 1446 7. Don't post anything that you don't have permission to post. For instance,  
1447 if you didn't write the material you are posting, make sure you have the  
1448 permission of the person who wrote it *before* you post it.
- 1449 8. On shameless advertising: Occasionally during the course of a discussion it  
1450 may be appropriate for a you to mention a product or service with which  
1451 you are involved if it helps the discussion and doesn't annoy anyone. We  
1452 will use our discretion in those cases.
- 1453 9. If we don't like what you post, or fear you may not have permission to  
1454 post it, we will remove it.
- 1455 10. If we keep having to remove your material, or if we *really* don't like it, we  
1456 will bar you from the forum.
- 1457 11. When you post material, you retain copyright but grant us the right to  
1458 use the material:

- 1459 • without payment,
  - 1460 • in any way we choose,
  - 1461 • anywhere in the world,
  - 1462 • forever.
- 1463 12. If we use your material, we will try to attribute it to you.
- 1464 13. If you wish to copy material posted by someone else, please contact us or  
1465 the person who posted for permission.

## 1466 Privacy and Data Protection

- 1467 14. We store any data that you submit to us, plus your IP address, details  
1468 about your browser and computer and which pages on our site you view.
- 1469 15. Our lawful basis for storing and using the data is ‘contract’. We store and  
1470 process this data in order to:
- 1471 • provide a discussion forum,
  - 1472 • monitor abuse,
  - 1473 • fix bugs
  - 1474 • and to improve our service.
- 1475 16. Your data is stored within the EU. Our processing is carried out within  
1476 the EU. Our forum is accessible from outside of the EU, so material you  
1477 post may be viewed from outside of the EU.
- 1478 17. Your forum account will lapse once your Tapestry subscription lapses or,  
1479 if you have a separate forum subscription directly or through your local  
1480 authority, once that subscription lapses.
- 1481 18. When your forum account lapses you will no longer be able to log into the  
1482 forum or post material to the forum. At our discretion, the material you  
1483 have posted may remain on the forum.
- 1484 19. When your forum account has lapsed we will only use the personal infor-  
1485 mation that you have provided us to:
- 1486 • help you re-activate your forum account if you later wish to re-  
1487 subscribe
  - 1488 • keep track of who posted what material in case we need to attribute  
1489 it to you or in case we need to verify that you had permission to post  
1490 the material.
- 1491 20. We will delete the personal information that you have provided us at most  
1492 7 years after your forum account has lapsed. At our discretion, the material  
1493 you have posted may remain on the forum.
- 1494 21. We are the data controller for this data. To exercise your rights under UK  
1495 data protection law you can contact us at [customer.service@eyfs.info](mailto:customer.service@eyfs.info).

- 1496 22. We have a Data Protection Officer, Lauren Foley, who can be reached at  
1497 dpo@eyfs.info.
- 1498 23. Our lead supervisory authority for data protection is the UK Information  
1499 Commissioner's Office (<https://ico.org.uk>).



## 1500 **Changes to this contract**

1501 Below is a list of material changes to this document. If you spot a change that  
1502 should be in this list, please let us know.

### 1503 **2018 May 1**

1504 Line numbers mentioned in this section are the line numbers marked on the PDF  
1505 copy of the 2018 May 1 version of this contract.

### 1506 **Tapestry Data Protection**

- 1507 • Add a section pointing out where to find in this contract the standard  
1508 terms required in a data processing agreement (lines 303-323)
- 1509 • Attempt to clarify the wording describing that viewing Tapestry from  
1510 outside the EU means data will be transferred outside the EU to get to  
1511 you (lines 351-358)
- 1512 • Rephrase “What data is placed into Tapestry?” to more closely match the  
1513 language of subject matter, nature and purpose, etc. that is used in data  
1514 protection legislation (lines 360-375)
- 1515 • Remove Bursar from the list of examples of who can instruct us (line 520).
- 1516 • Confirm that if someone who isn’t authorised tries to instruct us to do  
1517 something, we will tell you about it. (lines 525-526)
- 1518 • Clarify what ‘written’ instruction means (lines 530-540)
- 1519 • Added a section “Instructions we do and don’t accept” (lines 541-562).
- 1520 • Confirm that our staff who process data are appropriately trained in data  
1521 protection (line 568).
- 1522 • The tools to allow download of user’s data are now available (line 581).
- 1523 • Remove section “[NOT YET IMPLEMENTED We do provide some ex-  
1524 ample documents on risks that you can customise when carrying out your  
1525 own assessments. ]” – we have provided some guidance in our forum, but  
1526 not yet example documents (line 617).

### 1527 **Tapestry Security**

- 1528 • Remove the word ‘reset’ from links (line 847).
- 1529 • Clarify the wording that confirms connections between the Tapestry apps  
1530 and our servers are encrypted (line 938).
- 1531 • Change email to reach for keeping in touch about security. In urgent cases  
1532 we would call if we have appropriate contact details (line 1013).

**1533 Tapestry Privacy**

- 1534 • Remove the word ‘usually’. Our customers are always the data controllers  
1535 (line 1176)

**1536 Tapestry Sub Processor**

- 1537 • Remove the reference to Crashlytics, the forthcoming versions of the  
1538 Tapestry apps will no longer use this sub-processor (line 1153).

**1539 2018 March 12 (Second Draft)**

1540 Line numbers mentioned in this section are the line numbers marked on the PDF  
1541 copy of the 2018 March 12 draft.

**1542 Across all sections**

- 1543 • Fixed typos and improved some wording.
- 1544 • Adjust numbering that occurs because of other changes.
- 1545 • Make links to emails and websites clickable.

**1546 A note on this draft**

- 1547 • Mention the list of changes (line 163).
- 1548 • Fix dates (line 174).

**1549 Overview**

- 1550 • Clarify that we do sometimes call people back, and offer paid-for telephone  
1551 support sessions (lines 189-192).
- 1552 • State explicitly that we are GDPR compliant and this contract contains  
1553 the required clauses (lines 212-215).
- 1554 • State that the limit on liability is reciprocal (lines 268-269)
- 1555 • Clarify that some liabilities are set in law and we aren’t attempting to  
1556 override them (line 268). In particular, in relation to liabilities from  
1557 breaches in data protection law (lines 270-275).

**1558 Annex A: Tapestry Data Protection**

- 1559 • Provide more detail on where data is stored (lines 308-330).

- 1560 • Confirm that we won't change where data is stored without your agreement  
1561 (lines 309-311).
- 1562 • Reference the Privacy Policy for a fuller explanation of what data is covered  
1563 by this data processing agreement (line 345).
- 1564 • Confirm that we will get your *written* consent before changing our sub-  
1565 processors (line 363).
- 1566 • Confirm that we will tell you if we become aware of a breach (line 375, line  
1567 527, lines 578-582).
- 1568 • Suggest careful consideration of the lawful basis for adding data to Tapestry  
1569 (lines 384-387).
- 1570 • Expand on the implications of the right to be informed (lines 439-451).
- 1571 • Clarify we don't license your data (line 469).
- 1572 • Clarify who can tell you to restrict processing of data (it isn't us) (line  
1573 474).
- 1574 • Clarify who can instruct us (lines 480-493).
- 1575 • Confirm that we use sub-processors in a way that is compliant with data  
1576 protection law and point to the Annex for a description of how we will  
1577 seek your agreement if we wish to change them. (lines 505-507).
- 1578 • Clarify that we will help you to 'lock-down' your account if you suspect a  
1579 breach (line 531-534).
- 1580 • Clarify that you have to notify the data protection regulator in the case of  
1581 a breach (line 539).
- 1582 • Clarify we won't delete data if we are not allowed to by law (lines 562-563).
- 1583 • Clarify that we may partially or entirely lock down your account if we  
1584 suspect a breach (lines 583-587).
- 1585 • Add a FAQ on Brexit (lines 601-605).

## 1586 **Annex B: Tapestry Security**

- 1587 • Add VAT number (line 637)
- 1588 • Confirm that when data is deleted from our backups, it is no longer  
1589 recoverable by us (line 714).
- 1590 • Add a reminder about what to do if you suspect a password or email  
1591 account has been compromised (lines 795-803).
- 1592 • Clarify when and how we might store data on our local devices (lines  
1593 824-829).
- 1594 • Provide more detail on what our penetration tests cover (lines 906-912).
- 1595 • Confirm that we are insured (lines 969-972).
- 1596 • Make our TLS 1.0 support more obvious (lines 987-991).
- 1597 • Clarify that you can't force password changes every X days (lines 1078-  
1598 1083).
- 1599 • Confirm we have differentiated data access policies (lines 1095-1101).

**1600 Annex C: Tapestry Privacy**

- 1601 • Clarify that the Data Controller will need to add more information to fulfil  
1602 a subject's right to be informed (lines 1106-1113, lines 1153-1154).
- 1603 • Give examples of who 'you' might be (lines 1120-1121).
- 1604 • Clarify that we may contact 'managers' registered with Tapestry using the  
1605 contact details they have entered if we have a question or concern about  
1606 the associated Tapestry account (lines 1165-1167).
- 1607 • Clarify we also collect your IP address if you use our phone or tablet app  
1608 (line 1182).
- 1609 • Confirm that we do not share data about your computer or tablet (line  
1610 1193).
- 1611 • Clarify that the Data Controller will need to provide the lawful basis (line  
1612 1194-1197).
- 1613 • Remove troublesome reference to who owns data: keeping the fact that we  
1614 don't, but not claiming that you do (line 1199-1200).

**1615 Annex D: Tapestry Sub-processors**

- 1616 • Confirm that they are under a written contract with us (line 1266).
- 1617 • Confirm that we use them in a way that is consistent with this contract,  
1618 and give examples in relation to common questions. (lines 1271-1279).
- 1619 • Remove references to sub-processors we have now eliminated (line 1288).
- 1620 • Explain how we will seek your written consent if we need to add or change  
1621 sub-processors (lines 1290-1299).

**1622 Annex E: Billing and support data**

- 1623 • Explicitly state our lawful basis for processing data (line 1322).
- 1624 • Remove reference to United Hosting - we no longer use them (line 1330).
- 1625 • Clarify that we would share data relating to an account with other repre-  
1626 sentatives of that account. (lines 1334-1339).
- 1627 • Clarify that we do use your data to improve our service (line 1341).

**1628 Annex F: Use of our discussion forum**

- 1629 • Explicitly state our lawful basis for processing data (line 1405).

**1630 2018 January 5 (First draft)**

- 1631 • First public draft of new, more detailed, contract.