SAMPLE REPORT - FICTIONAL ORGANISATION

GOVERNANCE DOCS

# Privacy Risk Assessment

## Brightpath Learning (sample)

Learner, parent and staff personal data across the online learning platform, the support centre and the head office.

| | |
|---|---|
| ASSESSED | 25 September 2026 |
| METHOD | ISO/IEC 27701:2025, clauses 6.1.2 and 6.1.3, with GDPR Articles 24, 32 and 35 in mind |
| IN SCOPE | 11 scope items, 12 risks |
| APPETITE | Medium and below (level 9 or less) accepted without treatment |
| PROFILE | Education |
| PREPARED BY | Governance Docs |

Confidential. Prepared for Brightpath Learning (sample). Contains details of privacy risks, weaknesses in how personal data is handled and planned controls; share on a need-to-know basis.
Based on a self-assessment using information supplied by the organization. Not independently verified by Governance Docs; see "Basis of this report and limitation of liability".

CONTENTS

# Where the organization's risks stand

PROCESS SCORE

**88** / 100

## Level 2 · Developing

The risks are identified, but gaps in rating or treatment would not survive an audit.

Held at Developing while 1 critical finding is open; the score alone would place it higher.

Initial | **Developing** | Defined | Managed

The score measures how complete and defensible the assessment is, not how risky the organization is.

| RISKS | ABOVE APPETITE | CRITICAL | ABOVE AFTER TREATMENT | FINDINGS |
|---|---|---|---|---|
| 12 | 4 | 0 | 1 | 5 |

## WHAT THIS ASSESSMENT TELLS YOU

- 4 of 11 rated risks sit above your appetite line (Medium and below is acceptable).
- The highest risk is R-01, children's data collected without age checks or parental consent, at level 16 (High), owned by Data Protection Officer.
- 1 risk above the line has no treatment decision yet (R-05). Until it has one, the treatment plan is incomplete.
- Planned treatment brings the number of risks above the line from 4 to 1.
- 1 risk is not rated yet, so it is missing from the heat map and the priority order.

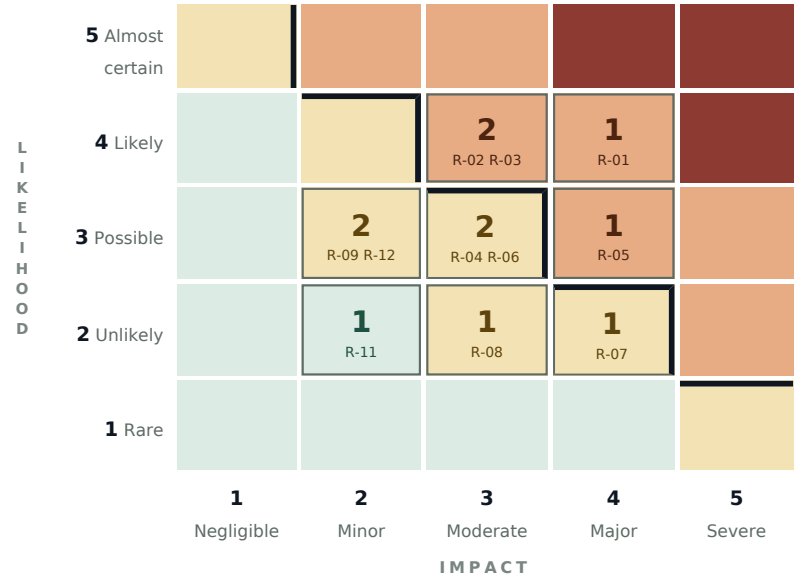
## DO THESE FIRST

| | SEVERITY | ACTION | RISKS | OWNER | DOCUMENT THAT CLOSES IT |
|---|---|---|---|---|---|
| 1 | CRITICAL | **Above the appetite line with no treatment decision**<br>Choose modify, avoid, share or retain for each one, with the risk owner. | R-05 | Legal Counsel | Risk treatment plan |
| 2 | MAJOR | **Scope item with no risks identified**<br>Link an existing risk to it, add a new one, or take it out of scope. | Employee HR records and CRM | To assign | Records of processing and risk register |

# Heat maps: today and after treatment

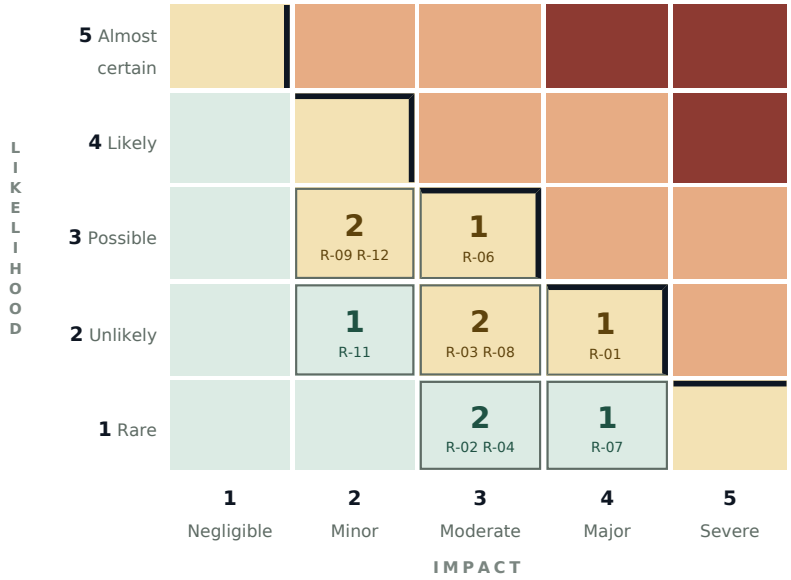
Each cell shows how many risks sit at that likelihood and impact, with their references. The heavy line is the appetite line: Medium and below (level 9 or less) is accepted without treatment. The second map shows where each risk is expected to be once its treatment is carried out; avoided risks are removed.

### Current risk levels




11 of 12 risks rated.

### Target levels after treatment




10 risks plotted; 0 removed by avoidance; risks above the line with no decision are not plotted.

Low 1–4 · Medium 5–9 · High 10–16 · Critical 17–25 · Appetite line

## RISKS BY LEVEL

| 1 Low | 6 Medium | 4 High | 1 Not rated |
|---|---|---|---|

# Analysis and priorities

**IN ONE SENTENCE**

**The register covers most of your processing; put a data processing agreement in place with the email marketing service before anything else.**

AI-assisted analysis, generated from the information the organization provided and checked automatically against the scores and findings in this report. It supports planning and is not an audit opinion; see "Basis of this report and limitation of liability".

**FOR SENIOR MANAGEMENT AND THE BOARD**

Our privacy risk assessment is largely complete: 12 risks identified, 4 above our appetite line, and treatment planned that brings that number to 1. One decision is outstanding. We need a treatment decision on the email marketing service, which processes learner data without a data processing agreement. With that decision recorded and two small gaps in the register closed, the assessment is ready for management review.

## WHERE YOU STAND

You have identified 12 privacy risks across 11 scope items, and 11 are rated. Your process score is 88 out of 100, but the level is held at Developing because one risk above your appetite line, processors used without a data processing agreement, has no treatment decision. The rest of the method is largely in place: criteria are defined, owners are named for all but one risk, and every treated risk has a target, an owner and a due date.

## WHAT IT MEANS FOR THE ORGANIZATION

4 risks sit above your appetite line, all of them High, and they share a pattern: personal data collected or kept without the controls the law expects, from children's accounts without parental consent to trackers that load before anyone agrees to them. If these materialise, the people most affected are learners and their parents, and the organization faces complaints and regulator attention at the same time. Your planned treatment brings the number above the line from 4 to 1.

## WHERE TO FOCUS FIRST

Decide how to treat the missing processing agreement first, because it is what an auditor would raise and what holds the level back. Then close the gaps in the register itself: rate the profiling risk, give the privacy notice risk an owner, and add the two scope items with no risks, employee HR records and the CRM. Finally, collect the owner's acceptance for the retention risk once its target is agreed.

## PRIORITIES

| | PRIORITY | WHY IT MATTERS | FIRST STEP | START FROM | WITHIN |
|---|---|---|---|---|---|
| 1 | **Put a processing agreement in place with the email service**<br>R-05 Processors used without a data processing agreement · Above the appetite line with no treatment decision | This High risk sits above your appetite line with no decision, which leaves the treatment plan incomplete and holds the level at Developing. | Ask the email marketing service for its data processing agreement and record modify as the decision, with a target and due date. | Risk treatment plan | 30 DAYS |
| 2 | **Rate the profiling risk on the learning platform**<br>R-10 Automated decisions or profiling without safeguards · Not yet rated for likelihood and impact | An unrated risk has no level, so it is missing from the heat map and cannot be compared with the appetite line. | Rate likelihood and impact against your criteria, with a sentence of rationale on how recommendations use learner data. | Risk assessment and treatment methodology | 30 DAYS |
| 3 | **Name an owner for the privacy notice risk**<br>R-12 Privacy notice incomplete or out of date · Risk with no owner | ISO/IEC 27701 expects an accountable owner for every privacy risk, and the notice is out of step with the new tutoring service. | Assign the risk to the Data Protection Officer and schedule the notice update. | Risk assessment and treatment methodology | 30 DAYS |
| 4 | **Cover employee HR records and the CRM**<br>Scope item with no risks identified | Two scope items have no risks linked, so the register cannot show that the data in them has been assessed. | Link an existing risk to each item or add one, such as excess access to HR records. | Records of processing and risk register | 60 DAYS |
| 5 | **Record acceptance for the retention risk**<br>R-03 Personal data kept longer than necessary · Residual risk not yet accepted by the owner | Residual risk for retention is not yet accepted; a name and a date is enough to show the owner agreed the plan. | Ask the Data Protection Officer to approve the retention plan and record the acceptance. | Risk treatment plan | 60 DAYS |

## 30 / 60 / 90-DAY ROADMAP

### FIRST 30 DAYS

- Record a treatment decision and target for the processing agreement risk.
- Rate the profiling risk on the learning platform.
- Assign an owner to the privacy notice risk.

### DAYS 31 TO 60

- Link risks to employee HR records and the CRM.
- Collect residual-risk acceptance for data retention.
- Launch the parental consent and age check at sign-up.

### DAYS 61 TO 90

- Carry the selected ISO 27701 controls into the Statement of Applicability.
- Present the updated register and treatment plan at management review.

# What was in scope

The personal data, processing activity, system or application, processor or recipient, people with access and location the assessment covered, with their owners. How much confidentiality (C), integrity (I) and availability (A) of this personal data or processing matter, to the people it is about and to you. H high, M medium, L low.

| Type | Scope item | Owner | C | I | A | Risks |
|---|---|---|---|---|---|---|
| Personal data | **Learner accounts and progress data** | Data Protection Officer | H | M | M | 2 |
| Personal data | **Children's data** | Data Protection Officer | H | H | M | 1 |
| Personal data | **Employee HR records** | HR Manager | H | M | L | **0** |
| Processing activity | **Marketing and newsletters** | Marketing Manager | M | L | L | 1 |
| Processing activity | **Customer support** | Customer Service Manager | M | M | M | 2 |
| Processing activity | **Website analytics and cookies** | Marketing Manager | M | L | L | 1 |
| System or application | **Learning platform** | IT Manager | H | H | H | 4 |
| System or application | **CRM** | Marketing Manager | M | M | M | **0** |
| Processor or recipient | **Cloud hosting provider** | IT Manager | H | M | H | 2 |
| Processor or recipient | **Email marketing service** | Marketing Manager | M | L | L | 1 |
| People with access | **Customer service team** | Customer Service Manager | – | – | – | 3 |

# Risk register

Every risk, highest level first. Level = likelihood x impact, rated with the controls already in place. The rationale is the organization's own reason for the rating. The full scenario for each risk (threat, weakness and consequence) is in the workbook.

| # | Ref | Risk scenario | Scope items | CIA | Owner | Existing controls | L | I | Level | Rationale |
|---|---|---|---|---|---|---|---|---|---|---|
| 1 | R-01 | **Children's data collected without age checks or parental consent**<br>Weakness: No age assurance and no parental consent step | Children's data, Learning platform | C | Data Protection Officer | Date of birth asked at sign-up | 4 | 4 | 16 · High | Under-13s can sign up without a parent; around 8% of new accounts are children. |
| 2 | R-05 | **Processors used without a data processing agreement**<br>Weakness: No contract terms or checks before a processor is used | Email marketing service, Cloud hosting provider | C | Legal Counsel | Standard terms with the hosting provider | 3 | 4 | 12 · High | The email marketing service was set up on click-through terms with no processing agreement. |
| 3 | R-02 | **Cookies and trackers set without consent**<br>Weakness: No working consent management on the website | Website analytics and cookies | C | Marketing Manager | Cookie banner with an accept button only | 4 | 3 | 12 · High | Analytics and advertising tags load before any choice is made. |
| 4 | R-03 | **Personal data kept longer than necessary**<br>Weakness: No retention schedule, or one nobody enforces with deletion | Learner accounts and progress data, Learning platform | C | Data Protection Officer | Retention period stated in the privacy notice | 4 | 3 | 12 · High | Closed accounts since 2017 remain in the platform database. |
| 5 | R-04 | **Access requests answered late or incompletely**<br>Weakness: No request process, and data scattered across systems nobody has mapped | Customer support, Learner accounts and progress data | A | Customer Service Manager | Requests logged in the support desk | 3 | 3 | 9 · Medium | Two of last year's access requests went past the one-month deadline. |
| 6 | R-06 | **Staff can see personal data they do not need**<br>Weakness: Access not based on role and never reviewed; no logging of who looked | Customer service team, Learning platform | C | IT Manager | Role-based access in the platform | 3 | 3 | 9 · Medium | All support staff can see full learner records including parents' details. |

| | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|
| 7 | R-07 | **A personal data breach is not reported in time**<br>Weakness: No breach procedure; nobody knows the reporting deadline or who decides | **None linked** | CIA | Data Protection Officer | Incident procedure for security events | 2 | 4 | **8 · Medium** | The procedure does not mention the 72-hour regulator deadline. |
| 8 | R-08 | **Personal data transferred abroad without safeguards**<br>Weakness: Transfers not mapped; no transfer mechanism or assessment | Cloud hosting provider | C | Legal Counsel | Hosting in the EU region | 2 | 3 | **6 · Medium** | Support tickets are handled by a platform with US sub-processors. |
| 9 | R-09 | **Personal data sent to the wrong recipient**<br>Weakness: No checks on sending personal data; no secure transfer option | Customer service team, Customer support | C | Customer Service Manager | Awareness training at induction | 3 | 2 | **6 · Medium** | Three misdirected emails last year, none with sensitive data. |
| 10 | R-12 | **Privacy notice incomplete or out of date**<br>Weakness: No owner for the privacy notice and no review when processing changes | Marketing and newsletters | C | **None** | Privacy notice last updated 2023 | 3 | 2 | **6 · Medium** | The notice does not mention the new tutoring service. |
| 11 | R-11 | **Staff not trained on handling personal data**<br>Weakness: No privacy training, or a one-off at induction | Customer service team | C | HR Manager | Annual e-learning | 2 | 2 | **4 · Low** | Completion is 94%. |
| 12 | R-10 | **Automated decisions or profiling without safeguards**<br>Weakness: No human review, no explanation and no way to contest the decision | Learning platform | CI | Product Manager | | – | – | **Not rated** | |

# What will be done, by whom and by when

Every risk with a treatment decision, earliest due date first. The ISO 27701 Annex A controls listed are the ones the treatment relies on; they carry into the Statement of Applicability. Acceptance is the risk owner's approval of the plan and of the risk that remains.

| Ref | Risk | Decision | Planned actions | ISO 27701 Annex A controls | Owner and due date | Current to target | Accepted |
|---|---|---|---|---|---|---|---|
| R-07 | **A personal data breach is not reported in time**<br>Data Protection Officer | **Modify** | Add a breach assessment step and the reporting clock to the incident procedure. | A.3.11 Information security incident management planning and preparation<br>A.3.12 Response to information security incidents | Data Protection Officer<br>31 Oct 2026 | 8 · Medium → 4 · Low | Chief Executive<br>22 Sep 2026 |
| R-04 | **Access requests answered late or incompletely**<br>Customer Service Manager | **Modify** | A request procedure with a tracker and a search checklist for each system. | A.1.3.7 Access, correction or erasure<br>A.1.3.9 Providing copy of PII processed | Customer Service Manager<br>15 Nov 2026 | 9 · Medium → 3 · Low | Data Protection Officer<br>22 Sep 2026 |
| R-02 | **Cookies and trackers set without consent**<br>Marketing Manager | **Modify** | Replace the banner with a consent tool that blocks tags until consent. | A.1.2.4 Determine when and how consent is to be obtained<br>A.1.2.5 Obtain and record consent | Marketing Manager<br>30 Nov 2026 | 12 · High → 3 · Low | Chief Executive<br>22 Sep 2026 |
| R-01 | **Children's data collected without age checks or parental consent**<br>Data Protection Officer | **Modify** | Add parental consent for under-13s and an age check at sign-up. | A.1.2.4 Determine when and how consent is to be obtained<br>A.1.2.5 Obtain and record consent | Product Manager<br>15 Dec 2026 | 16 · High → 8 · Medium | Chief Executive<br>22 Sep 2026 |
| R-03 | **Personal data kept longer than necessary**<br>Data Protection Officer | **Modify** | Adopt a retention schedule and a quarterly deletion job. | A.1.4.8 Retention<br>A.1.4.9 Disposal | IT Manager<br>31 Jan 2027 | 12 · High → 6 · Medium | **Not recorded** |

| | | | | | | |
|---|---|---|---|---|---|---|
| R-06 | **Staff can see personal data they do not need**<br>IT Manager | **Retain** | Risk retained at its current level. | – | 9 · Medium → 9 · Medium | **Not recorded** |

## ABOVE THE LINE WITH NO DECISION YET

| Ref | Risk | Owner | Level |
|---|---|---|---|
| R-05 | **Processors used without a data processing agreement** | Legal Counsel | 12 · High |

4 risks are within appetite (Medium and below) and need no treatment; 1 are not yet rated.

# Where the assessment falls short

Each finding is a gap between the assessment as recorded and what ISO 27701 clauses 6.1.2 and 6.1.3 ask for, with the risks it applies to and the document that closes it.

| Severity | Finding | Applies to | What it means | To fix | Document that closes it |
|---|---|---|---|---|---|
| CRITICAL | **Above the appetite line with no treatment decision** | R-05 | These risks are rated above Medium, the highest level you accept without treatment, but nobody has decided what to do about them. ISO 27701 expects a treatment option to be chosen for every risk that fails the acceptance criteria. | Choose modify, avoid, share or retain for each one, with the risk owner. | Risk treatment plan |
| MAJOR | **Scope item with no risks identified** | Employee HR records and CRM | Something you put in scope has no risk attached to it. Either it faces no credible risk, which is rare, or the identification step missed it. | Link an existing risk to it, add a new one, or take it out of scope. | Records of processing and risk register |
| MAJOR | **Not yet rated for likelihood and impact** | R-10 | Without both ratings a risk has no level, so it cannot be compared with the appetite line or placed in priority order. | Rate each one against the likelihood and impact scales in your criteria. | Risk assessment and treatment methodology |
| MAJOR | **Risk with no owner** | R-12 | ISO/IEC 27701 requires a risk owner for every privacy risk: the person with the accountability and authority to manage it. | Name an owner, by role, for each risk. | Risk assessment and treatment methodology |
| MINOR | **Residual risk not yet accepted by the owner** | R-03 | ISO/IEC 27701 asks risk owners to approve the treatment plan and accept the privacy risk that remains. A name and a date is enough to show it happened. | Record the owner's acceptance once they have approved the plan. | Risk treatment plan |

## PROCESS SCORE IN DETAIL

| | | | |
|---|---|---|---|
| **Criteria defined**<br>Every likelihood and impact level has a definition, and the appetite line is set. | 100% | 11 of 11 | weight 10 |
| **Scope covered**<br>Every scope item has at least one risk linked to it. | 82% | 9 of 11 | weight 10 |
| **Risk owners named**<br>Every risk has an owner accountable for it. | 92% | 11 of 12 | weight 15 |
| **Risks rated**<br>Every risk has a likelihood and an impact, so it has a level. | 92% | 11 of 12 | weight 15 |
| **Ratings explained**<br>Existing controls and a rationale are recorded for each risk. | 92% | 22 of 24 | weight 10 |
| **Treatment decided**<br>Every risk above the appetite line has a treatment option chosen. | 75% | 3 of 4 | weight 15 |
| **Targets within appetite**<br>Treatments bring each risk to a target at or below the line. | 100% | 3 of 3 | weight 10 |
| **Treatments scheduled**<br>Each treatment has an owner and a due date. | 100% | 3 of 3 | weight 5 |
| **Residual risk accepted**<br>Risk owners have accepted what remains after treatment, by name and date. | 67% | 2 of 3 | weight 10 |

**Findings by severity**


**1 · Initial (0+)**

A start on a register, not yet an assessment that decisions can rest on.

**2 · Developing (40+)**

The risks are identified, but gaps in rating or treatment would not survive an audit.

**3 · Defined (60+)**

A complete, repeatable assessment with a treatment plan behind it.

**4 · Managed (80+)**

Owned, justified and accepted: ready for management review and audit.

A · APPENDIX

# Criteria used and basis of this report

ISO/IEC 27701 clause 6.1.2 asks for privacy risk criteria, including acceptance criteria, that give consistent, valid and comparable results, and that weigh the consequences for the people whose data it is as well as for the organization. This is the record of the criteria every rating in this report was made against.

## LIKELIHOOD SCALE

| Value | Label | Definition |
|---|---|---|
| 1 | **Rare** | Not expected in the next 5 years; no known case here or in the sector |
| 2 | **Unlikely** | Could happen once in 2 to 5 years; has happened in the sector |
| 3 | **Possible** | Could happen about once a year |
| 4 | **Likely** | Expected several times a year |
| 5 | **Almost certain** | Expected monthly or more often, or already happening |

## IMPACT SCALE

| Value | Label | Definition |
|---|---|---|
| 1 | **Negligible** | No noticeable effect on the people concerned; under 10,000 |
| 2 | **Minor** | Minor inconvenience to a limited group; internal escalation; 10,000 to 50,000 |
| 3 | **Moderate** | Distress or inconvenience for many people; complaints; possible regulator query |
| 4 | **Major** | Significant harm to people; reportable breach; media interest; 250,000 to 1 million |
| 5 | **Severe** | Serious, lasting or irreversible harm to people; enforcement; over 1 million |

## RISK LEVELS AND ACCEPTANCE

| Band | Levels | Treatment |
|---|---|---|
| Low | 1–4 | Accepted without treatment |
| Medium | 5–9 | Accepted without treatment |
| High | 10–16 | Needs a treatment decision |
| Critical | 17–25 | Needs a treatment decision |

Level = likelihood x impact. A risk above the appetite line may still be retained, but only with the risk owner's recorded acceptance.

**Process score.** Nine dimensions, each the share of risks (or of risks above the line) that meet it, multiplied by its weight; the weights add up to 100. A dimension with nothing in scope counts in full. Any critical finding holds the level at Developing, whatever the score.

**Your workbook.** The Excel workbook that comes with this report is the register as a working file. Change a likelihood or impact on the Risk register sheet and every level, the heat maps on the Dashboard and the process score recalculate. It also holds the treatment plan and a Statement of Applicability starter listing the ISO 27701 Annex A controls your treatments rely on.

### BASIS OF THIS REPORT AND LIMITATION OF LIABILITY

This report is the output of a self-assessment. The risks, ratings, risk levels, treatment decisions, findings, analysis and recommendations in this report are derived solely from the information entered by the organization, and have not been independently reviewed, verified, tested or audited by Governance Docs. Governance Docs did not conduct an independent assessment of the organization, its controls or its operations.

The accuracy and completeness of the results depend entirely on the accuracy and completeness of the information provided. Governance Docs gives no assurance, certification or audit opinion, and accepts no liability for any inaccuracy, omission or deviation arising from that information, or for any decision taken, or not taken, in reliance on this report.

The report, including any AI-assisted analysis, is provided for guidance and planning only. It does not constitute legal, regulatory or other professional advice, and it does not replace an independent assessment or a certification audit.

Privacy risk assessment for Brightpath Learning (sample), generated 25 September 2026 by Governance Docs. This is a structured self-assessment based on the organization's own criteria and ratings. It is not a certification, an audit opinion or a substitute for an independent risk assessment.