

DATA PROCESSING ADDENDUM

ReportBox Ltd

Version 1.0

Introduction

This Data Processing Addendum ("DPA") forms part of the agreement between ReportBox Ltd ("ReportBox") and the Customer for the provision of the ReportBox online reporting platform and related services ("Services").

This DPA sets out the responsibilities of each party in relation to the processing of Personal Data and forms part of the contractual arrangements between ReportBox and the Customer.

This DPA is intended to satisfy the requirements of Article 28 of the UK General Data Protection Regulation ("UK GDPR") and the Data Protection Act 2018.

This DPA should be read alongside the ReportBox Privacy Policy (<https://www.reportbox.com/privacy>), which explains how ReportBox processes personal data where it acts as a Data Controller.

1. Purpose and Scope

1.1

This Data Processing Addendum ("DPA") forms part of the agreement between ReportBox Ltd ("ReportBox") and the Customer for the provision of the ReportBox online reporting platform and related services ("Services").

1.2

This DPA applies whenever ReportBox processes Personal Data on behalf of the Customer in connection with the Services.

1.3

The purpose of this DPA is to set out the responsibilities of each party in relation to the processing of Personal Data and to ensure compliance with Applicable Data Protection Law.

1.4

This DPA is intended to satisfy the requirements of Article 28 of the UK General Data Protection Regulation ("UK GDPR") and the Data Protection Act 2018.

1.5

If there is any conflict between this DPA and the main service agreement, this DPA shall prevail only to the extent necessary to satisfy Applicable Data Protection Law.

2. Definitions

2.1

Unless otherwise defined in this DPA, capitalised terms shall have the meanings given to them in the main service agreement.

2.2

For the purposes of this DPA:

Applicable Data Protection Law means the UK General Data Protection Regulation, the Data Protection Act 2018 and any legislation replacing or supplementing those laws.

Controller, Processor, Processing, Personal Data, Data Subject, Personal Data Breach and **Special Category Data** have the meanings given to them in Applicable Data Protection Law.

Customer Data means any Personal Data processed by ReportBox on behalf of the Customer in connection with the Services.

Sub-processor means any third party engaged by ReportBox to process Customer Data on its behalf.

3. Roles of the Parties

3.1

The Customer acts as the Controller of the Personal Data processed under this DPA.

3.2

ReportBox acts as the Processor of Customer Data and shall process Personal Data only on behalf of the Customer.

3.3

Nothing in this DPA transfers ownership of Customer Data to ReportBox.

3.4

The Customer is responsible for:

- determining the purposes and lawful basis for processing Personal Data;
- ensuring that Personal Data is collected lawfully;
- providing any required privacy information to Data Subjects; and
- complying with its obligations as Controller under Applicable Data Protection Law.

3.5

ReportBox shall process Personal Data only:

- in accordance with this DPA;
- in accordance with the Customer's documented instructions;
- as necessary to provide the Services; or
- where required by Applicable Data Protection Law.

3.6

Where ReportBox is required by law to process Personal Data other than in accordance with the Customer's instructions, ReportBox shall notify the Customer before carrying out such processing unless prohibited from doing so by law.

4. Processing of Personal Data

4.1

ReportBox shall process Personal Data only on behalf of the Customer and only for the purposes of providing the Services described in the Agreement.

4.2

ReportBox shall process Personal Data only:

- in accordance with the Customer's documented instructions;
- as necessary to provide, maintain, support and secure the Services;
- as required to comply with Applicable Data Protection Law.

4.3

If ReportBox reasonably believes that an instruction from the Customer infringes Applicable Data Protection Law, ReportBox shall inform the Customer without undue delay before carrying out the instruction, unless prohibited from doing so by law.

4.4

ReportBox shall not:

- sell Customer Data;
- use Customer Data for advertising or marketing purposes;
- disclose Customer Data to any third party except as permitted by this DPA or required by law.

4.5

ReportBox may process Personal Data for its own legitimate business purposes only where it acts as an independent Controller, including for:

- financial accounting;
- tax compliance;
- legal and regulatory obligations;
- fraud prevention;
- maintaining the security and integrity of its systems.

Such processing shall not include the use of Customer Data for profiling, marketing or commercial exploitation.

4.6

The Customer may provide additional written instructions relating to the processing of Personal Data, provided those instructions:

- are consistent with this DPA;
- are technically feasible;
- do not materially alter the nature of the Services.

Where additional instructions require significant development work or materially increase ReportBox's costs, the parties shall agree any associated charges before the work is undertaken.

4.7

ReportBox shall comply with Applicable Data Protection Law in carrying out the processing described in this DPA.

4.8

ReportBox shall maintain records of processing activities where required by Applicable Data Protection Law.

4.9

ReportBox shall provide reasonable assistance to the Customer to enable it to comply with its obligations under Applicable Data Protection Law, including in relation to:

- Data Subject Requests;
- Personal Data Breaches;
- Data Protection Impact Assessments;
- consultations with the Information Commissioner's Office.

Where the assistance requested falls outside the normal operation of the Services and requires substantial additional work, ReportBox may charge reasonable fees, provided these are agreed with the Customer in advance.

5. Confidentiality and Personnel

5.1

ReportBox shall ensure that all employees, contractors and other personnel authorised to process Personal Data are subject to appropriate contractual or statutory duties of confidentiality.

5.2

ReportBox shall ensure that authorised personnel:

- access Personal Data only where necessary to perform their duties;
- receive appropriate training in data protection and information security;
- understand the confidential nature of Customer Data;
- comply with ReportBox's internal security policies and procedures.

5.3

ReportBox shall maintain appropriate procedures to manage user access, including the granting, review and removal of access rights where appropriate.

5.4

ReportBox shall take reasonable steps to ensure that only authorised personnel have access to Customer Data.

5.5

The obligations contained within this clause shall continue after an individual ceases to work for or provide services to ReportBox.

6. Technical and Organisational Security Measures

6.1

ReportBox shall implement and maintain appropriate technical and organisational measures designed to protect Personal Data against accidental or unlawful destruction, loss, alteration, unauthorised disclosure or access.

6.2

In determining appropriate security measures, ReportBox shall take account of:

- the nature of the Personal Data;
- the risks presented by the processing;
- the state of technological development;
- the cost of implementation;
- the likelihood and severity of potential harm to Data Subjects.

6.3

Security measures maintained by ReportBox may include, where appropriate:

- encryption of data in transit;
- secure cloud hosting;
- role-based access controls;
- authentication of authorised users;
- secure password management;
- logging and monitoring of administrative activity;
- regular software updates and security patches;
- backup and disaster recovery procedures;

- malware protection;
- secure software development practices.

6.4

ReportBox shall regularly review the effectiveness of its security measures and update them where appropriate to reflect changes in technology, threats and industry practice.

6.5

ReportBox shall maintain appropriate business continuity and disaster recovery arrangements designed to minimise disruption to the Services.

6.6

Where Customer Data is backed up, ReportBox shall implement reasonable measures to protect backup data from unauthorised access and accidental loss.

6.7

Nothing in this DPA requires ReportBox to undertake independent penetration testing, obtain security certification or provide proprietary security documentation unless separately agreed in writing.

7. Personal Data Breaches

7.1

ReportBox shall maintain procedures for identifying, investigating, managing and responding to Personal Data Breaches affecting Customer Data.

7.2

Upon becoming aware of a Personal Data Breach affecting Customer Data, ReportBox shall notify the Customer without undue delay and in any case within 24 hours.

7.3

The notification shall include, where reasonably available:

- the nature of the Personal Data Breach;
- the categories of Personal Data affected;
- the likely consequences of the breach;
- the measures taken, or proposed to be taken, to contain and remedy the breach;

- the name and contact details of the person responsible for managing the incident.

7.4

Where all relevant information is not available at the time of notification, ReportBox shall provide additional information as it becomes available.

7.5

ReportBox shall cooperate with the Customer in investigating the breach and in meeting the Customer's obligations under Applicable Data Protection Law.

7.6

Unless required by law, ReportBox shall not notify any Data Subject, regulator or third party regarding a Personal Data Breach affecting Customer Data without first consulting the Customer.

8. Sub-processors

8.1

The Customer provides general authorisation for ReportBox to appoint Sub-processors to assist in delivering the Services.

8.2

ReportBox shall ensure that each Sub-processor is engaged under a written agreement imposing data protection obligations that are no less protective than those contained within this DPA.

8.3

ReportBox remains responsible for the acts and omissions of its Sub-processors in relation to the processing of Customer Data.

8.4

ReportBox shall maintain an up-to-date list of Sub-processors, which shall form **Schedule 3** of this DPA.

8.5

Where ReportBox proposes to appoint a new Sub-processor that may process Customer Data, ReportBox shall update Schedule 3 and provide reasonable notice to affected Customers.

8.6

If the Customer has reasonable data protection concerns regarding a proposed Sub-processor, the Customer may notify ReportBox in writing within thirty (30) days of receiving notice.

The parties shall work together in good faith to address those concerns.

8.7

If no reasonable solution can be agreed, either party may terminate the affected Services by written notice without penalty.

9. International Transfers

9.1

ReportBox shall store and process Customer Data within the United Kingdom or European Union wherever reasonably practicable.

9.2

Where Customer Data is transferred outside the United Kingdom, ReportBox shall ensure that appropriate safeguards are implemented in accordance with Applicable Data Protection Law.

9.3

Such safeguards may include:

- an adequacy decision;
- the UK International Data Transfer Agreement (IDTA);
- the UK Addendum to the EU Standard Contractual Clauses; or
- any other lawful transfer mechanism recognised under Applicable Data Protection Law.

9.4

ReportBox shall provide reasonable information regarding international transfers upon written request.

10. Data Subject Rights

10.1

Taking account of the nature of the processing, ReportBox shall provide reasonable assistance to enable the Customer to respond to requests from Data Subjects exercising their rights under Applicable Data Protection Law.

10.2

If ReportBox receives a request directly from a Data Subject relating to Customer Data, ReportBox shall:

- promptly notify the Customer;
- not respond directly unless authorised by the Customer or required by law;
- provide reasonable assistance to the Customer where required.

10.3

Where reasonably requested, ReportBox shall assist the Customer in responding to requests concerning:

- access;
- rectification;
- erasure;
- restriction of processing;
- objection to processing;
- data portability.

10.4

ReportBox shall notify the Customer without undue delay if it receives:

- correspondence from the Information Commissioner's Office;
- correspondence from another supervisory authority;
- complaints relating to Customer Data;
- legal requests requiring disclosure of Customer Data.

11. Freedom of Information

11.1

The parties acknowledge that many Customers are subject to the Freedom of Information Act 2000.

11.2

If ReportBox receives a request under the Freedom of Information Act relating to Customer Data or the Services provided to the Customer, ReportBox shall promptly notify the Customer.

11.3

ReportBox shall not respond directly to such requests unless authorised by the Customer or required by law.

11.4

ReportBox shall provide reasonable assistance to enable the Customer to comply with its obligations under the Freedom of Information Act.

12. Audit and Compliance

12.1

ReportBox shall maintain records and documentation reasonably necessary to demonstrate its compliance with this DPA and Applicable Data Protection Law.

12.2

Upon reasonable written request, and no more than once in any twelve (12) month period unless required by law or following a Personal Data Breach, ReportBox shall provide the Customer with reasonable information to demonstrate compliance with this DPA.

12.3

Such information may include, where appropriate:

- copies of relevant policies and procedures;
- details of technical and organisational security measures;
- responses to reasonable security questionnaires;
- information regarding Sub-processors;
- confirmation of compliance with applicable legal obligations.

12.4

Where the information provided is not reasonably sufficient to demonstrate compliance, the Customer may request a remote audit.

12.5

Any audit shall:

- be conducted during normal business hours;
- be subject to reasonable notice;
- avoid unnecessary disruption to ReportBox's business;
- protect the confidentiality and security of other customers and ReportBox's confidential information.

12.6

Nothing in this DPA requires ReportBox to:

- permit unrestricted physical access to its premises;
- provide access to systems belonging to third-party hosting providers;
- disclose confidential information relating to other customers;
- disclose information that would compromise the security of the Services.

12.7

Where an audit reveals a material failure to comply with this DPA, ReportBox shall promptly take reasonable steps to remedy the issue.

13. Retention and Deletion

13.1

ReportBox shall retain Customer Data only for as long as necessary to provide the Services or as otherwise required by law.

13.2

During the term of the Agreement, the Customer may access and export Customer Data using the functionality provided within the Services or by requesting reasonable assistance from ReportBox.

13.3

Following termination of the Agreement, ReportBox shall retain Customer Data for up to two years to enable Customers to return more easily unless:

- the Customer requests earlier deletion;
- the parties agree a longer retention period;

- retention is required by law.

13.4

At the end of the applicable retention period, ReportBox shall securely delete or anonymise Customer Data unless continued retention is required by law.

13.5

Backup copies containing Customer Data shall be securely overwritten or deleted in accordance with ReportBox's normal backup retention procedures.

13.6

Upon written request, ReportBox shall provide reasonable confirmation that Customer Data has been deleted in accordance with this clause.

14. Liability

14.1

Each party shall remain responsible for complying with its respective obligations under Applicable Data Protection Law.

14.2

Nothing in this DPA excludes or limits either party's liability where such liability cannot lawfully be excluded or limited.

14.3

Subject to Clause 14.2, ReportBox's total aggregate liability arising under or in connection with this DPA shall not exceed the total fees paid by the Customer to ReportBox during the twelve (12) months immediately preceding the event giving rise to the claim.

14.4

Neither party shall be liable to the other for:

- indirect loss;
- consequential loss;
- loss of profits;
- loss of anticipated savings;

- loss of goodwill,

except where such limitation is prohibited by law.

14.5

Each party shall take reasonable steps to mitigate any losses arising from a breach of this DPA.

15. Term and Termination

15.1

This DPA shall commence on the date the Agreement comes into effect and shall remain in force for as long as ReportBox processes Personal Data on behalf of the Customer.

15.2

Termination of the Agreement shall automatically terminate this DPA, subject to the obligations relating to deletion, confidentiality and any obligations that are intended to survive termination.

15.3

Either party may terminate this DPA immediately if continued performance would result in a breach of Applicable Data Protection Law.

16. Variation

16.1

ReportBox may update this DPA where necessary to:

- reflect changes in Applicable Data Protection Law;
- reflect changes to the Services;
- reflect changes to ReportBox's security practices;
- maintain compliance with regulatory guidance.

16.2

Where a change materially reduces the protections provided to the Customer, ReportBox shall provide reasonable prior notice.

16.3

Any other amendment to this DPA shall be made in writing and agreed by both parties.

17. Governing Law

17.1

This DPA shall be governed by and interpreted in accordance with the laws of Northern Ireland.

17.2

The courts of Northern Ireland shall have non-exclusive jurisdiction in relation to any dispute arising from or connected with this DPA.

Schedule 1 – Details of Processing

Description	Details
Controller	Customer
Processor	ReportBox Ltd
Purpose of Processing	Provision of the ReportBox online pupil reporting platform.
Subject Matter	Collection, storage, organisation, retrieval, transmission and deletion of educational records.

Duration	For the duration of the Customer's subscription and any applicable retention period.
Categories of Data Subjects	Pupils, teachers, school staff and, where applicable, parents or guardians.
Categories of Personal Data	Names, classes, year groups, assessment information, teacher comments, user accounts, email addresses and other information entered by the Customer.
Special Category Data	Not intentionally processed unless entered by the Customer.
Processing Activities	Hosting, storage, retrieval, backup, support, transmission and deletion.

Schedule 2 – Technical and Organisational Measures

ReportBox maintains appropriate technical and organisational measures designed to protect Customer Data, including where appropriate:

- secure cloud hosting;
- encryption of data in transit;
- authenticated user access;
- role-based permissions;
- password management;
- secure administrative access;
- regular software updates;
- vulnerability management;
- malware protection;
- logging and monitoring;
- backup and disaster recovery procedures;
- staff confidentiality obligations;
- staff training;

- secure software development practices;
- incident management procedures;
- periodic review of security controls.

Security measures are reviewed periodically and updated where appropriate to reflect changes in technology, threats and industry practice.

Schedule 3 – Approved Sub-processors

ReportBox may use the following categories of Sub-processors in delivering the Services:

Supplier	Purpose	Data Location
AWS (Ireland)	Hosting of the application and databases	Ireland
Sinch Mailgun	Transactional email delivery	UK or approved jurisdiction
Backup provider	AWS & Google Cloud	UK or approved jurisdiction
Sunflower Learning Ltd	Technical Support	United Kingdom
Atto Partners	Software Development	United Kingdom

ReportBox shall maintain an up-to-date list of Sub-processors and make it available to Customers upon request or via its website.