Red Balloon Educational Trust - Norfolk

Data Protection Policy

Effective date:	6th February 2024
Review date:	5th February 2025
Reviewed by:	Sarah Saunders
Approved by:	

Red Balloon Educational Trust - Norfolk
76 Earlham Road, Norwich NR2 3DF
Tel: 01603 327856 • **www.redballoonlearner.org** • Email: sarah.saunders@rbet.ac

Founder and President: Carrie Herbert MBE
Registered Charity No. 1109606. Company Registered in England and Wales No. 05385341

Contents

1. Introduction

Red Balloon Educational Trust - Norfolk is committed to protecting the rights and freedoms of data subjects (natural persons) by ensuring the safe and secure processing of their data in accordance with Data Protection Legislation.

Data Protection Legislation means the Data Protection Act 2018 (DPA2018), United Kingdom General Data Protection Regulation (UK GDPR), the Privacy and Electronic Communications (EC Directive) Regulations 2003 and any legislation implemented in connection with the aforementioned legislation. Where data is processed by a controller or processor established in the European Union or comprises the data of people in the European Union, it also includes the EU General Data Protection Regulation (EU GDPR). This includes any replacement legislation coming into effect from time to time. We hold personal data about our employees, clients, suppliers and other individuals for a variety of business purposes.

This policy sets out how we seek to protect personal data and ensure that our employees understand the rules governing their use of the Personal Data to which they have access during their work.

In particular, this policy requires staff to ensure that the relevant Centre GDPR Lead be consulted before any significant new data processing activity is initiated to ensure that the relevant compliance steps are taken and approved by the Red Balloon Educational Trust Data Protection Officer (DPO).

Red Balloon Educational Trust – Norfolk's senior leadership team is fully committed to ensuring continued and effective implementation of this policy and expects all employees to share in this commitment. Any breach of this policy will be taken seriously and may result in disciplinary action.

2. Definitions

Personal data	'Personal data' means any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person. *Personal data we gather may include: individuals' phone number, email address, educational background, financial and pay details, details of certificates and diplomas, education and skills, marital status, nationality, job title, and CV.*

Special categories of personal data	Special categories of data include information about an individual's racial or ethnic origin, political opinions, religious or similar beliefs, trade union membership (or non-membership), physical or mental health or condition, criminal offences or related proceedings, and genetic and biometric information —any use of special categories of personal data should be strictly controlled in accordance with this policy.

Data controller	'Data controller' means the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data; where the purposes and means of such processing are determined by law, the controller or the specific criteria for its nomination may be provided for by said law.
Data processor	'Processor' means a natural or legal person, public authority, agency or other body, which processes personal data on behalf of the controller.
Processing	'Processing' means any operation or set of operations which is performed on personal data, or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.
Supervisory authority	This is the national body responsible for data protection. The supervisory authority for our organisation is the Information Commissioner's Office (ICO).

3. Scope

This policy applies to all processing of personal data whether:

- wholly or partly by automated means (i.e.by computer), or
- by other means (i.e. paper records) that form part of filing system or are intended to form part of a filing system.

This policy applies to all staff and anyone else working on our behalf including contractors and agency staff, who must be familiar with this policy and comply with its terms.

This policy supplements our other policies such as those relating to internet and email use. We may supplement or amend this policy by additional policies and

guidelines from time to time. Any new or modified policy will be circulated to staff before being implemented.

4. Purpose

The purpose of this policy is to provide guidance on the data protection principles that all those acting on behalf of Red Balloon Educational Trust – Norfolk must adhere to when any personal data belonging to or provided by data subjects is collected, stored or transmitted.

It is therefore imperative that all those who access this policy, including employees, contractors, and vendors, comply with the Seven Data Protection Principles, summarised below.

Personal Data (information identifying a living person) should:

1) Be processed fairly, lawfully and transparently
2) Be collected and processed only for specified, explicit and legitimate purposes
3) Be adequate, relevant and limited to what is necessary for the purposes for which it is processed
4) Be kept accurate and up to date. Any inaccurate data must be deleted or rectified without delay
5) Be kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the data are processed
6) Be processed in a manner that ensures appropriate security, using appropriate technical and organisational measures
7) Data controllers must be responsible for, and be able to demonstrate compliance with, the above principles (Accountability Principle).

Accountability and transparency

We must ensure accountability and transparency in all our use of personal data.

Data protection legislation obliges all employees to take a proactive approach to data protection.

In order to encourage best practice – and to avoid penalties from the Information Commissioner's Office (ICO) – all employees are required to read this policy, to treat others' personal data with due care and consideration, and to ensure that the organisation is able to demonstrate compliance.

5. Our Procedures

We must process personal data fairly and lawfully in accordance with individuals' rights under the first Principle. At least one lawful basis (explained below) must apply.

If we cannot apply a lawful basis, our processing does not conform to the first principle and will be unlawful. Data subjects have the right to stop the processing of any personal data that has been unlawfully processed and have it erased.

Controlling vs. Processing data

Red Balloon Educational Trust – Norfolk is classified as a data controller. We must maintain our appropriate registration with the Information Commissioner's Office in order to continue lawfully controlling data.

As a Data Controller, we remain ultimately liable for all of our data processing activities complying with Data Protection Legislation. This means that we must take responsibility for the compliance of our Data Processors as well as our own actions.

As a Data Controller, we must:

- Demonstrate the highest level of compliance responsibility
- Comply and demonstrate compliance with all Data Protection Principles as well as the other GDPR and Data Protection Act 2018 requirements
- Co-operate fully with the ICO or other supervisory authority
- Manage data breaches and Data Subjects' rights requests efficiently and within specified time frames
- Pay the data protection registration fee

Lawful basis for processing data

When processing any personal data (information which does or may identify a living individual), we must establish a lawful basis for processing data. Employees must ensure that any data they are responsible for managing or working with has a written lawful basis approved by the Red Balloon Educational Trust DPO.

At least one of the following conditions must apply whenever we process personal data:

1. **Consent**
   We hold recent, clear, explicit, and defined consent for the individual's data to be processed for a specific purpose.
2. **Contract**
   Processing is necessary to fulfil or prepare a contract for the individual.
3. **Legal obligation**
   Processing is necessary to meet a legal obligation (excluding a contract).
4. **Vital interests**
   Processing is necessary to protect a person's life or in an urgent medical situation.

5. **Public task**
   Processing is necessary to carry out a public function, a task of public interest, or the function has a clear basis in law assigned to us.
6. **Legitimate interest**
   Processing is necessary for the business/organisation's legitimate interests. This condition does not apply if there is a good reason to protect the individual's personal data which overrides the legitimate interest.

Deciding which condition to rely on

If you are making an assessment of the lawful basis of processing, you must first establish that the processing is necessary to achieve your purpose. This means the processing must be a targeted, appropriate way of achieving a stated purpose. You cannot rely on a lawful basis if you can reasonably achieve the same purpose by some other means that doesn't require the use of the personal data. You must also only use the minimum data required to achieve the purpose (e.g. don't use a full date of birth if an age or age range will do).

Remember that more than one basis may apply, and you should rely on what will best fit the purpose, not what is easiest.

Consider the following factors and document your answers:

- What is the purpose for processing the data?
- Can it reasonably be done in a different way?
- Is there a choice as to whether or not to process the data?
- Who does the processing benefit?
- After selecting the lawful basis, is this the same as the lawful basis the data subject would expect?
- What is the impact of the processing on the individual?
- Are you in a position of power over them?
- Are they a vulnerable person?
- Would they be likely to object to the processing?
- Are you able to stop the processing at any time on request, and have you factored in how to do this?

Our commitment to the first Principle requires us to document this process and show that we have considered which lawful basis best applies to each processing purpose, and fully justify these decisions. All data processing must be recorded reported to and recorded by the Red Balloon Educational Trust DPO.

We must also ensure that individuals whose data is being processed by us are informed of the lawful basis for processing their data, as well as the intended purpose. This should occur via a Privacy Notice. This applies whether we have collected the data directly from the individual, or from another source. You must

record how individuals are to be informed and for written communications keep a copy of the wording used.

If no other lawful basis applies, you may be able to rely on Legitimate Interests. If this is the case a Legitimate Interests Assessment (LIA) must be undertaken and documented. If you need to conduct an LIA, you must conduct the Red Balloon Educational Trust DPO who will assist in conducting and approving the assessment. Note that in most cases, Legitimate Interests is only likely to be a suitable legal basis where the processing has little likelihood of affecting the rights or freedoms of a data subject.

6. Special Categories of Personal Data

What are special categories of personal data?

Previously known as sensitive personal data, special category data is data about an individual which is more sensitive, so requires more protection. This type of data could create more significant risks to a person's fundamental rights and freedoms, for example by putting them at risk of unlawful discrimination. The special categories include information about an individual's:

- race
- ethnic origin
- politics including political opinions and party support or membership
- religion
- philosophy
- trade union membership
- genetics
- biometrics (where used for ID purposes)
- health
- sexual orientation

In most cases where we process special categories of personal data, we will require the data subject's explicit consent to do this unless exceptional circumstances apply, or we are required to do this by law (e.g. to comply with legal obligations to ensure health and safety at work). Any such consent will need to clearly identify what the relevant data is, why it is being processed and to whom it will be disclosed.

The condition for processing special categories of personal data must comply with the law. If we do not have a lawful basis for processing special categories of data that processing activity must cease.

Criminal record checks

Any criminal record checks undertaken must be justified in law. Criminal record checks cannot be undertaken based solely on the consent of the subject. We cannot keep a comprehensive register of criminal offence data. All data relating to criminal offences is considered to be a special category of personal data and must be treated as such. You must have approval prior to carrying out a criminal record check or processing data relating to criminal records to ensure this is lawful.

7. Responsibilities

Our responsibilities

- Analysing and documenting the type of personal data we hold
- Checking procedures to ensure they cover all the rights of the individual
- Identify the lawful basis for processing data
- Ensuring consent procedures are lawful
- Implementing and reviewing procedures to detect, report and investigate personal data breaches
- Storing data in safe and secure ways
- Assessing the risk that could be posed to individuals' rights and freedoms should data be compromised

Your responsibilities

- Fully understand your data protection obligations
- Check that any data processing activities you are dealing with comply with our policy and are justified
- Not to use data in any unlawful way
- Not to store data incorrectly, be careless with it or otherwise cause us to breach data protection laws and our policies through your actions
- Comply with this policy at all times
- Raise any concerns, use internal reporting procedures to notify of any breaches or errors, and report anything suspicious or contradictory to this policy or our legal obligations without delay

Accuracy and relevance

We will ensure that any personal data we process is accurate, adequate, relevant and not excessive, given the purpose for which it was obtained. We will not process personal data obtained for one purpose for any unconnected purpose unless the individual concerned has agreed to this or would otherwise reasonably expect this.

If you aren't clear the purpose for which data was collected but wish to use it, or you wish to use it for another purpose, you must seek approval from the Red Balloon Educational Trust DPO who can confirm the purpose for which the data was collected and whether and proposed new purpose is compatible. Where the proposed use is significantly different, involves combining data from different sources, or otherwise might have a significant impact on data subjects, a Data Protection Impact Assessment may need to be undertaken.

Individuals may ask that we correct inaccurate personal data relating to them. If you believe that information is inaccurate you should record the fact that the accuracy of the information is disputed and escalate internally.

Data security

You must keep personal data secure against loss or misuse. Where other organisations process personal data as a service on our behalf, the Red Balloon Educational Trust DPO will recommend what, if any, additional specific data security arrangements need to be implemented in contracts with those third-party organisations.

Storing data securely

- In cases where data is stored on printed paper, it should be kept in a secure place where unauthorised personnel cannot access it
- Printed data should be shredded when it is no longer needed
- Data stored on a computer should be protected by strong passwords that are changed regularly. We encourage all staff to use a password manager to create and store their passwords
- Data stored on CDs or memory sticks must be encrypted or password protected and locked away securely when they are not being used
- The Red Balloon Educational Trust DPO must approve any cloud used to store data in collaboration with the IT Department and any external consultants.
- Servers containing personal data must be kept in a secure location, away from general office space
- Data should be regularly backed up in line with the company's backup procedures
- Data should never be saved directly to mobile devices such as laptops, tablets or smartphones
- All servers containing sensitive data must be approved and protected by security software
- All possible technical measures must be put in place to keep data secure

Data retention

We must retain personal data for no longer than is necessary. What is necessary will depend on the circumstances of each case, taking into account the reasons that the personal data was obtained, but should be determined in a manner consistent with our data retention guidelines. If you are responsible for any data, you must ensure that an appropriate retention period is applied and is documented within the retention schedule.

Transferring data internationally

There are restrictions on international transfers of personal data. You must not transfer personal data abroad, or anywhere else outside of normal rules and procedures, without consulting with the Red Balloon Educational Trust DPO.

8. Rights of Individuals

Individuals have rights to their data which we must respect and comply with to the best of our ability. We must ensure individuals can exercise their rights in the following ways:

1. Right to be informed

- We will provide privacy notices which are concise, transparent, intelligible and easily accessible, free of charge, that are written in clear and plain language, particularly if aimed at children.
- We must keep a record of how we use personal data to demonstrate compliance with the need for accountability and transparency.

2. Right of access (Subject Access Requests)

- We will enable individuals to access their personal data and supplementary information.
- We will allow individuals to be aware of and verify the lawfulness of the processing activities.

3. Right to rectification

- We will rectify or amend the personal data of an individual if requested because it is inaccurate or incomplete.
- This will be done without delay, and no later than one month from the request. This can be extended to two months with permission from the Red Balloon Educational Trust DPO.

4. Right to erasure

- We will delete or remove an individual's data if requested and there is no compelling reason for its continued processing.

5. Right to restrict processing

- We will comply with any request to restrict, block, or otherwise suppress the processing of personal data.
- We are permitted to store personal data if it has been restricted, but not process it further. We must retain enough data to ensure the right to restriction is respected in the future.

6. Right to data portability

- We will provide individuals with their data so that they can reuse it for their own purposes or across different services where we process it on the basis of consent or contractual obligation.
- We will provide it in a commonly used, machine-readable format, and send it directly to another controller if requested.

7. Right to object

- We will respect the right of an individual to object to data processing based on legitimate interest or the performance of a public interest task unless there is an overriding reason to continue the processing.
- We will respect the right of an individual to object to direct marketing, including profiling and will cease if an objection is received.
- We will respect the right of an individual to object to processing their data for scientific and historical research and statistics.

8. Rights in relation to automated decision making and profiling

- We will respect the rights of individuals in relation to automated decision making and profiling.
- Individuals retain their right to object to such automated processing, have the rationale explained to them, and request human intervention.

9. Privacy Notices

When to supply a privacy notice

A privacy notice must be supplied at the time the data is obtained if obtained directly from the data subject. If the data is not obtained directly from the data subject, the privacy notice must be provided within a reasonable period of having obtained the data, which means within one month or at the time the data is first processed, whichever is sooner.

If the data is being used to communicate with the individual, then the privacy notice must be supplied when the first communication takes place at the latest.

If disclosure to another recipient is envisaged, then the privacy notice must be supplied prior to the data being disclosed.

What to include in a privacy notice

Privacy notices must be concise, transparent, intelligible and easily accessible. They are provided free of charge and must be written in clear and plain language, particularly if aimed at children.

The following information must be included in a privacy notice to all data subjects:

- Identification and contact information of the data controller and the Red Balloon Educational Trust DPO
- The purpose of processing the data and the lawful basis for doing so
- The legitimate interests of the controller or third party, if applicable
- The right to withdraw consent at any time, if applicable
- The category of the personal data (only for data not obtained directly from the data subject)
- Any recipient or categories of recipients of the personal data
- Detailed information about any transfers to third countries and the safeguards in place
- The retention period of the data or the criteria used to determine the retention period, including details for the data disposal after the retention period
- The right to lodge a complaint with the ICO, and internal complaint procedures
- The source of the personal data, and whether it came from publicly available sources (only for data not obtained directly from the data subject)
- Any existence of automated decision making, including profiling, and information about how those decisions are made, their significances and consequences to the data subject
- Whether the provision of personal data is part of a statutory or contractual requirement or obligation and possible consequences for any failure to provide the data (only for data obtained directly from the data subject)

At a minimum, all initial contact with data subjects, or those which will require a new collection of or reason for processing data, must make reference to the relevant Privacy Notice.

- Where you are collecting new data or processing it in a new way you must seek advice from the Red Balloon Educational Trust DPO.

10. Subject Access Requests

What is a subject access request?

An individual has the right to receive confirmation that their data is being processed and have access to their personal data. For further information regarding these requests, please see the Red Balloon Educational Trust Data Subject Access Request (DSAR) Policy.

How we deal with subject access requests

- We must provide the individual with a copy of the information they requested, free of charge. This must occur without delay, and within one month of receipt of the request. We endeavour to provide data subjects access to their information in commonly used electronic formats, and where possible, provide direct access to the information through a remote accessed secure system.
- If complying with the request is complex or numerous, the deadline can be extended by two months, but the individual must be informed within one month. You must obtain approval from the Red Balloon Educational Trust DPO before extending the deadline.
- We can refuse to respond to certain requests, and can, in circumstances of the request being manifestly unfounded or excessive, charge a fee. If the request is for a large quantity of data, we can request the individual specify the information they are requesting.
- Once a subject access request has been made, you must not change or amend any of the data that has been requested. Doing so is a criminal offence.

11. Right to Erasure

What is the right to erasure?

Individuals have a right to have their data erased and for processing to cease in the following circumstances:

- Where the personal data is no longer necessary in relation to the purpose for which it was originally collected and / or processed
- Where consent is withdrawn

- Where the individual objects to processing and there is no overriding legitimate interest for continuing the processing
- Where the personal data was unlawfully processed or otherwise breached data protection laws
- To comply with a legal obligation

How we deal with the right to erasure

We can only refuse to comply with a right to erasure in the following circumstances:

- To exercise the right of freedom of expression and information
- To comply with a legal obligation, for the performance of a public interest task or exercise of official authority
- For public health purposes in the public interest
- For archiving purposes in the public interest, scientific research, historical research or statistical purposes
- For the exercise or defence of legal claims

If personal data that needs to be erased has been passed onto other parties or recipients, they must be contacted and informed of their obligation to erase the data. If the individual asks, we must inform them of those recipients.

The right to object

Individuals have the right to object to their data being used on grounds relating to their particular situation. We must cease processing unless:

- We have legitimate grounds for processing which override the interests, rights and freedoms of the individual
- The processing relates to the establishment, exercise or defence of legal claims

We must always inform the individual of their right to object at the first point of communication, i.e. in the privacy notice. We must offer a way for individuals to object online.

The right to restrict automated profiling or decision making

We may only carry out automated profiling or decision making that has a legal or similarly significant effect on an individual in the following circumstances:

- It is necessary for the entry into or performance of a contract
- We have gained the individual’s explicit consent

- We are otherwise authorised by law

In these circumstances, we must:

- Give individuals detailed information about the automated processing
- Offer simple ways for them to request human intervention or challenge any decision about them
- Carry out regular checks and user testing to ensure our systems are working as intended

12. Third parties

Using third party data processors

As a data controller, we must have written contracts in place with any third-party data processors that we use. The contract must contain specific clauses which set out our and their liabilities, obligations and responsibilities.

As a data controller, we must only appoint processors who can provide sufficient guarantees under the UK GDPR that the rights of data subjects will be respected and protected.

Contracts

Our contracts must comply with the minimum contractual requirements set out in the UK GDPR. Our contracts with data processors must set out the subject matter and duration of the processing, the nature and stated purpose of the processing activities, the types of personal data and categories of data subject, and the obligations and rights of the controller.

At a minimum, our contracts must include terms that specify:

- The processor will act only on written instructions
- Those involved in processing the data are subject to a duty of confidence
- Appropriate measures will be taken to ensure the security of the processing
- Sub-processors will only be engaged with the prior consent of the controller and under a written contract
- The controller will assist the processor in dealing with subject access requests and allowing data subjects to exercise their rights under UK GDPR
- The processor will assist the controller in meeting its UK GDPR obligations in relation to the security of processing, notification of data breaches and performance of Data Protection Impact Assessments
- The processor(s) and sub-processor(s) will delete or return all personal data at the end of the contract

- Both the processor and the controller will submit to regular audits and inspections, and provide whatever information necessary for the controller and processor to meet their legal obligations
- Nothing will be done by either the controller or processor to infringe on UK GDPR

13. Audits, Monitoring and Training

Data audits

Regular data audits to manage and mitigate risks will be carried out. This includes information on what data is held, where it is stored, how it is used, who is responsible and any further regulations or retention timescales that may be relevant. You must conduct a regular data audit as required by the Red Balloon Educational Trust DPO and normal procedures.

Monitoring

Everyone must observe this policy. The Red Balloon Educational Trust DPO has overall responsibility for updating this policy. Red Balloon Educational Trust - Norfolk will keep this policy under review and amend or change it as required. You must notify the Red Balloon Educational Trust DPO of any breaches of this policy. You must comply with this policy fully and at all times.

Training

You will receive adequate training on provisions of data protection law relevant to your role. You must complete all training as requested. If you move role or responsibilities, you are responsible for requesting new data protection training relevant to your new role or responsibilities.

If you require additional training on data protection matters, contact the Red Balloon Educational Trust DPO.

14. Reporting Breaches

Any breach of this policy or of data protection laws must be reported as soon as practically possible. This means as soon as you have become aware of a breach. For externally reportable breaches, we have a legal obligation to report the data breach to the Information Commissioners Office (ICO) within 72 hours.

All members of staff have an obligation to report actual or potential data protection compliance failures. This allows us to:

- Investigate the failure and take remedial steps if necessary
- Maintain a register of compliance failures

- Notify the ICO of any compliance failures that are material either in their own right or as part of a pattern of failures

Any member of staff who fails to notify the relevant person of a breach or is found to have known or suspected a breach has occurred but has not followed the correct reporting procedures will be liable to disciplinary action.

Please refer to our Data Breach Policy for our reporting procedure.

15. Compliance

The importance of this policy means that failure to comply with any requirement may lead to disciplinary action under our procedures, which may result in dismissal.

Questions about the interpretation or operation of this policy should be taken up in the first instance with the relevant Centre GDPR Lead who will collaborate with the Red Balloon Educational Trust DPO where required.

Any individual who considers that the Policy has not been followed in respect of Personal Data about themselves should also raise the matter with the GDPR Lead.

Further information about the DPA ‘18 and the UK GDPR can be found on the Information Commissioner’s Office (ICO) website: **https://ico.org.uk/.**