Data Management Policy and Procedures (GDPR)

Bouncing Statistics

Overcoming the misunderstood conception

Policy Prepared:	Rackeem Reid
Required on the website:	No
Policy became operational on:	01/09/2025
Revision Date	01/09/2026
Signed by:	R.Reid

Introduction:

Bouncing Statistics is a research-led educational organization providing culturally competent training, mentoring, and tutoring to bridge the educational gap for marginalized communities. We work directly with schools, pupils, parents, and teachers across the West Midlands to close the opportunity gap through:
- Mentoring and tutoring for pupils
- Inclusion support and inclusion hubs
- Teacher training and CPD
- Parent workshops and family engagement
- Strategic consultancy for schools and MATs

As a result Bouncing Statistics needs to gather and use certain information about individuals.

These can include schools, suppliers, business contacts, employees and other people the organisation has a relationship with or may need to contact.

This policy describes how this personal data must be collected, handled and stored to meet the company's data protection standards – and to comply with the law.

Why this policy exists:

This data management policy ensures Bouncing Statistics:

- Complies with data protection law and follows good practice
- Protects the rights of customers, staff and partners
- Is transparent about how it stores and processes individuals' data
- Protects itself from the risks of a data breach

Data protection law:

The General Data Protection Regulation (GDPR) applies in the UK and across the EU from May 2018. It requires personal data shall be:

1. Processed lawfully, fairly and in a transparent manner in relation to individuals;
2. Collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research or statistical purposes shall not be considered to be incompatible with the initial purposes;

3. Adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed;
4. Accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay;
5. Kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes subject to implementation of the appropriate technical and organisational measures required by GDPR in order to safeguard the rights and freedoms of individuals;
6. Processed in a manner that ensures appropriate security of personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.
7. The controller shall be responsible for, and be able to demonstrate, compliance with the principles.

   In addition to this there are further regulatory requirements which have an impact upon organisations like Bouncing Statistics and how they should operate.

   1. ICO Data Protection Audit Framework (October 2024)

   - Nine specialised audit toolkits now available
   - Enhanced compliance monitoring requirements
   - Specific guidance for educational organisations

   2. EU AI Act Implementation (August 2024)

   - New obligations for AI systems in educational settings
   - Enhanced transparency requirements for automated decision-making
   - Specific protections for AI processing of children's data

   3. EDPB Opinion 28/2024 on AI Models (December 2024)

   - Case-by-case anonymity assessments required
   - Three-step test for legitimate interest in AI contexts
   - Enhanced consent requirements for AI processing

   4. Enhanced Children's Data Protection Requirements

   - Stricter protections for under-16 data processing
   - Enhanced parental consent mechanisms
   - Age-appropriate design requirements

People and responsibilities

Everyone at Bouncing Statistics contributes to compliance with GDPR. We understand that key decision makers must understand the requirements and accountability of the organisation sufficiently to prioritise and support the implementation of compliance. The following responsibilities are undertaken and maintained by Bouncing Statistics:

- Keeping senior management updated about data protection issues, risks and responsibilities
- Documenting, maintaining, and developing the organisation's data protection policy and related procedures, in line with agreed schedule
- Embedding ongoing privacy measures into corporate policies and day-to-day activities, throughout the organisation and within each business unit that processes personal data. The policies themselves will stand as proof of compliance
- Dissemination of policy across the organisation, and arranging training and advice for staff
- Dealing with subject access requests, deletion requests and queries from clients, stakeholders, and data subjects about data protection related matters
- Checking and approving contracts or agreements with third parties that may handle the company's sensitive data
- Ensuring all systems, services and equipment used for storing data meet acceptable security standards
- Performing regular checks and scans to ensure security hardware and software is functioning properly
- Evaluating any third-party services, the company is considering using to store or process data, to ensure their compliance with obligations under the regulations
- Developing privacy notices to reflect lawful basis for fair processing, ensuring that intended uses are clearly articulated, and that data subjects understand how they can give or withdraw consent, or else otherwise exercise their rights in relation to the company's use of their data
- Ensuring that audience development, marketing, fundraising and all other initiatives involving processing personal information and/or contacting individuals abide by the GDPR principles
- Implementing and monitoring ICO Data Protection Audit Framework toolkits
- Conducting AI impact assessments for any automated systems
- Ensuring enhanced protections for children's data processing (under-16s)
- Managing multi-agency data sharing arrangements with schools and local
- authorities
- Coordinating safeguarding information sharing protocols
- Monitoring compliance with AI Act requirements for educational technology
- Conducting quarterly self-assessments using ICO audit toolkits

Data Protection Officer (DPO) – the person responsible for fulfilling the tasks of the DPO in respect of Bouncing Statistics is Rackeem Reid.

The tasks of the DPO are:

- To inform and advise the organisation and its employees about their obligations to comply with the GDPR and other data protection laws
- To monitor compliance with the GDPR and other data protection laws, including managing internal data protection activities, advise on data protection impact assessments; train staff and conduct internal audits
- To be the first point of contact for supervisory authorities and for individuals whose data is processed (employees, customers etc)
- To monitor compliance with AI Act requirements for educational systems
- To oversee implementation of ICO audit framework toolkits
- To conduct enhanced children's data protection assessments
- To coordinate with schools and local authorities on data sharing compliance
- To manage AI transparency and notification requirements
- To ensure age-appropriate design compliance for digital services

Staff are responsible for:

- Collecting, storing and processing any personal data in accordance with this policy
- Informing Bouncing Statistics of any changes to their personal data, such as a change of address
- Contacting the DPO in the following circumstances:

o With any questions about the operation of this policy, data protection law, retaining personal data or keeping personal data secure
o If they have any concerns that this policy is not being followed
o If they are unsure whether or not they have a lawful basis to use personal data in a particular way
o If they need to rely on or capture consent, draft a privacy notice, deal with data protection rights invoked by an individual, or transfer personal data outside the European Economic Area
o If there has been a data breach
o Whenever they are engaging in a new activity that may affect the privacy rights of individuals
o If they need help with any contracts or sharing personal data with third parties

Scope of personal information to be processed

We will only process personal data where we have one of 6 ‘lawful bases’ (legal reasons) to do so under data protection law:

- The data needs to be processed so that Bouncing Statistics can **fulfil a contract** with the individual, or the individual has asked the school to take specific steps before entering into a contract
- The data needs to be processed so that Bouncing Statistics can **comply with a legal obligation**
- The data needs to be processed to ensure the **vital interests** of the individual e.g. to protect someone’s life
- The data needs to be processed so that Bouncing Statistics, as a public authority, can perform a task **in the public interest,** and carry out its official functions

- The data needs to be processed for the **legitimate interests** of Bouncing Statistics or a third party (provided the individual's rights and freedoms are not overridden)
- The individual (or their parent/carer when appropriate in the case of a pupil) has freely given clear **consent.**
- For special categories of personal data, we will also meet one of the special category conditions for processing which are set out in the GDPR and Data Protection Act 2018.
- If we offer online services to pupils, such as apps, and we intend to rely on consent as a basis for processing, we will get parental consent where the pupil is under 16 (except for online counselling and preventive services).
- Whenever we first collect personal data directly from individuals, we will provide them with the relevant information required by data protection law.

When considering what constitutes a lawful basis it is necessary to continue to take into the context of Bouncing Statistics educational context.

For pupil mentoring and support services:

- Legitimate interests: Providing educational support and mentoring to improve outcomes
- Consent: Where pupils/parents agree to specific mentoring programmes
- Public task: Where working with schools/local authorities on statutory duties

For Safeguarding Activities:

- Vital interests: Protecting pupil welfare and safety
- Legal obligation: Statutory safeguarding reporting requirements
- Public task: Multi-agency safeguarding responsibilities

For Parent/Family Engagement:

- Consent: Workshop participation and family support programs
- Legitimate interests: Educational engagement and community support

For School Partnership Working:

- Public task: Supporting educational outcomes and statutory school functions
- Legitimate interests: Collaborative educational service delivery

Limitation, minimisation and accuracy

We will only collect personal data for specified, explicit and legitimate reasons. We will explain these reasons to the individuals when we first collect their data.

If we want to use personal data for reasons other than those given when we first obtained it, we will inform the individuals concerned before we do so and seek consent where necessary.

Staff must only process personal data where it is necessary in order to do their jobs. When staff no longer need the personal data they hold, they must ensure it is deleted or anonymised. This will be done in accordance with Bouncing Statistics Record Retention Policy.

Photographs and videos

As part of our activities, we may take photographs and record images of individuals.

We will obtain written consent from parents/carers, for pupils aged 18 and under, for photographs and videos to be taken of pupils for communication, marketing and promotional materials.

Where we need parental consent, we will clearly explain how the photograph and/or video will be used to both the parent/carer and pupil. Where we don't need parental consent, we will clearly explain to the pupil how the photograph and/or video will be used.

Uses may include:

- External agencies such as the photographer, newspapers, campaigns
- Online on our website or social media pages
- Consent can be refused or withdrawn at any time. If consent is withdrawn, we will delete the photograph or video and not distribute it further.
- When using photographs and videos in this way we will not accompany them with any other personal information about the child, to ensure they cannot be identified.
- See our child protection and safeguarding policy/photography policy/other relevant policy for more information on our use of photographs and videos.

Data protection by design and default

We will put measures in place to show that we have integrated data protection into all of our data processing activities, including:

- Appointing a suitably qualified DPO, and ensuring they have the necessary resources to fulfil their duties and maintain their expert knowledge
- Only processing personal data that is necessary for each specific purpose of processing, and always in line with the data protection principles set out in relevant data protection law
- Completing privacy impact assessments where processing of personal data presents a high risk to rights and freedoms of individuals, and when introducing new technologies (the DPO will advise on this process)
- Integrating data protection into internal documents including this policy, any related policies and privacy notices

- Regularly training members of staff on data protection law, this policy, any related policies and any other data protection matters; we will also keep a record of attendance
- Regularly conducting reviews and audits to test our privacy measures and make sure we are compliant
- Maintaining records of our processing activities, including:

o For the benefit of data subjects, making available the name and contact details of our organisation and DPO and all information we are required to share about how we use and process their personal data (via our privacy notices)

o For all personal data that we hold, maintaining an internal record of the type of data, data subject, how and why we are using the data, any third-party recipients, how and why we are storing the data, retention periods and how we are keeping the data secure

AI System Inventory and Assessment:

- Maintain register of all AI systems and automated decision-making tools
- Conduct AI impact assessments for educational technology
- Implement transparency notifications for AI interactions
- Enhanced consent procedures for AI processing of children's data

For Automated Decision-Making Safeguards:

- There are human oversight requirements for decisions affecting pupils
- Right to explanation for automated educational assessments
- Enhanced protections for vulnerable young people
- Regular review of algorithmic fairness and bias

ICO Audit Framework Compliance:
- Quarterly Self-Assessment Requirements:
- Age-Appropriate Design Toolkit (Priority 1 for educational organisations)
- Training and Awareness Toolkit implementation
- Data Sharing Toolkit for school partnerships
- Artificial Intelligence Toolkit for any automated systems
- Personal Data Breach Management Toolkit updates

Compliance Monitoring:
- Monthly compliance dashboard reporting
- Quarterly toolkit-based assessments
- Annual comprehensive compliance review
- Regulatory change monitoring and implementation

Data security and storage of records

We will protect personal data and keep it safe from unauthorised or unlawful access, alteration, processing or disclosure, and against accidental or unlawful loss, destruction or damage.

In particular:

- Paper-based records and portable electronic devices, such as laptops and hard drives that contain personal data are kept under lock and key when not in use
- Papers containing confidential personal data must not be left on office and classroom desks, on staffroom tables, pinned to notice/display boards, or left anywhere else where there is general access
- Where personal information needs to be taken off site, staff must sign it in and out from the school office, whilst informing their supervisor and the DPO
- Passwords must be at least 12 characters long with complexity requirements only these are used to access company computers, laptops and other electronic devices. Staff and pupils are reminded to change their passwords at regular intervals
- Encryption software is used to protect all portable devices and removable media, such as laptops and USB devices
- In the event that staff should store personal information on their personal devices, they are expected to follow the same security procedures as for company-owned equipment
- Where we need to share personal data with a third party, we carry out due diligence and take reasonable steps to ensure it is stored securely and adequately protected.

Disposal of Records

Personal data that is no longer needed will be disposed of securely. Personal data that has become inaccurate or out of date will also be disposed of securely, where we cannot or do not need to rectify or update it. For example, we will shred or incinerate paper-based records, and overwrite or delete electronic files. We may also use a third party to safely dispose of records on the organisation's behalf. If we do so, we will require the third party to provide sufficient guarantees that it complies with data protection law. All personal data will be retained and disposed of in line with Bouncing Statistics' Record Retention Policy.

Personal data breaches

The company will make all reasonable endeavours to ensure that there are no personal data breaches. In the unlikely event of a suspected data breach, we will follow the procedure set out in appendix 1.

- Safeguarding information being made available to an unauthorised person.
- The theft of a company laptop containing non-encrypted personal data about pupils.

Training

All staff are provided with data protection training as part of their induction process.

Data protection will also form part of continuing professional development, where changes to legislation, guidance or the school's processes make it necessary.

Monitoring arrangements

The DPO is responsible for monitoring and reviewing this policy.

This policy will be reviewed and updated if necessary when the Data Protection Bill receives royal assent and becomes law (as the Data Protection Act 2018) – if any changes are made to the bill that affect our school's practice. Otherwise, or from then on, this policy will be comprehensively reviewed **every year** and shared with the full governing board.

Subject access requests

Individuals are entitled to ask what information the organisation holds about them and why, how to gain access to it, who it is shared with, how it is kept up to date, and how the organisation is meeting its data protection obligations. The organisation will respond to subject access requests within one month, in line with UK GDPR requirements. Where requests are complex, this may be extended by a further two months, with the individual notified within the first month.

Staff should contact the DPO to request the data held by the company. Employees will be provided with this data in a private meeting with the DPO.

Ongoing documentation of measures to ensure compliance

Meeting the obligations of the GDPR to ensure compliance will be an ongoing process. Bouncing Statistics details here the ongoing measures implemented to:

1. Maintain documentation/evidence of the privacy measures implemented and records of compliance
2. Regularly test the privacy measures implemented and maintain records of the testing and outcomes.
3. Use the results of testing, other audits, or metrics to demonstrate both existing and continuous compliance improvement efforts.
4. Keep records showing training of employees on privacy and data protection matters.

Appendix 1: Personal data breach procedure

This procedure is based on 'guidance on personal data breaches' produced by the ICO.

- On finding or causing a breach, or potential breach, the staff member or data processor must immediately notify the DPO

- The DPO will investigate the report, and determine whether a breach has occurred. To decide, the DPO will consider whether personal data has been accidentally or unlawfully:

  o Lost
  o Stolen
  o Destroyed
  o Altered
  o Disclosed or made available where it should not have been

  o Made available to unauthorised people

- The DPO will raise with the other director and record this within the management meeting.
- The DPO will make all reasonable efforts to contain and minimise the impact of the breach, assisted by relevant staff members or data processors where necessary. (Actions relevant to specific data types are set out at the end of this procedure).
- The DPO will assess the potential consequences, based on how serious they are, and how likely they are to happen.
- The DPO will work out whether the breach must be reported to the ICO. This must be judged on a case-by-case basis. To decide, the DPO will consider whether the breach is likely to negatively affect people's rights and freedoms, and cause them any physical, material or non-material damage (e.g. emotional distress), including through:

  o Loss of control over their data o Discrimination
  o Identify theft or fraud
  o Financial loss
  o Unauthorised reversal of pseudonymisation (for example, key-coding)
  o Damage to reputation
  o Loss of confidentiality
  o Any other significant economic or social disadvantage to the individual(s) concerned

  If it's likely that there will be a risk to people's rights and freedoms, the DPO must notify the ICO.

  Some further examples of high-risk scenario breaches are the following:

- Unauthorised access to pupil mentoring records
- Safeguarding information disclosure to unauthorised parties
- Parent/guardian contact details shared inappropriately
- School partnership data sharing breaches
- Educational technology platform security incidents
- Multi-agency information sharing protocol failures
- Automated decision-making system failures affecting pupils
- AI model data extraction or inference attacks
- Algorithmic bias incidents in educational assessments
- Unauthorised AI processing of children's data

- Educational technology AI system compromises

- The DPO will document the decision (either way), in case it is challenged at a later date by the ICO or an individual affected by the breach. Documented decisions are stored on the company's computer system.
- Where the ICO must be notified, the DPO will do this via the 'report a breach' page of the ICO website within 72 hours. As required, the DPO will set out:

  o A description of the nature of the personal data breach including, where possible:

▪ The categories and approximate number of individuals concerned

▪ The categories and approximate number of personal data records concerned

▪ The name and contact details of the DPO

▪ A description of the likely consequences of the personal data breach

▪ A description of the measures that have been, or will be taken, to deal with the breach and mitigate any possible adverse effects on the individual(s) concerned

- If all the above details are not yet known, the DPO will report as much as they can within 72 hours. The report will explain that there is a delay, the reasons why, and when the DPO expects to have further information. The DPO will submit the remaining information as soon as possible
- The DPO will also assess the risk to individuals, again based on the severity and likelihood of potential or actual impact. If the risk is high, the DPO will promptly inform, in writing, all individuals whose personal data has been breached. This notification will set out:

o The name and contact details of the DPO

o A description of the likely consequences of the personal data breach

o A description of the measures that have been, or will be, taken to deal with the data breach and mitigate any possible adverse effects on the individual(s) concerned

- The DPO will notify any relevant third parties who can help mitigate the loss to individuals – for example, the police, insurers, banks or credit card companies
- The DPO will document each breach, irrespective of whether it is reported to the ICO. For each breach, this record will include the:

o Facts and cause

o Effects

o Action taken to contain it and ensure it does not happen again (such as establishing more robust processes or providing further training for individuals)

Records of all breaches will be stored on the company's computer system.

The DPO will meet with co-CEO to review what happened and how it can be stopped from happening again. This meeting will happen as soon as is reasonably possible

Actions to minimise the impact of data breaches

We will take the actions set out below to mitigate the impact of different types of data breach, focusing especially on breaches involving particularly risky or sensitive information. We will review the effectiveness of these actions and amend them as necessary after any data breach.

Sensitive information being disclosed via email (including safeguarding records)

- If special category data (sensitive information) is accidentally made available via email to unauthorised individuals, the sender must attempt to recall the email as soon as they become aware of the error
- Members of staff who receive personal data sent in error must alert the sender and the DPO as soon as they become aware of the error
- If the sender is unavailable or cannot recall the email for any reason, the DPO will ask the ICT department to recall it
- In any cases where the recall is unsuccessful, the DPO will contact the relevant unauthorised individuals who received the email, explain that the information was sent in error, and request that those individuals delete the information and do not share, publish, save or replicate it in any way.

- The DPO will ensure we receive a written response from all the individuals who received the data, confirming that they have complied with this request
- The DPO will carry out an internet search to check that the information has not been made public; if it has, we will contact the publisher/website owner or administrator to request that the information is removed from their website and deleted

Other types of breach that you might want to consider could include:

- Details of pupil premium interventions for named children being published on the company website
- Non-anonymised staff pay information being shared with staff
- A company laptop containing non-encrypted sensitive personal data being stolen or hacked.