Institute for Research in Schools
Data Protection Policy

October 2022

1. Introduction

IRIS is the Institute for Research in Schools ('we', 'us', 'our').

The security and management of data is important to ensure that we can function effectively and successfully for the benefit of students, schools, our partners and staff.

In doing so, it is essential that people's privacy is protected through the lawful and appropriate use and handling of their personal information.

The use of all personal data by IRIS is governed by:

- The General Data Protection Regulation (GDPR)
- The UK Data Protection Act 2018 (DPA)
- The Privacy and Electronic Communications Regulations (PECR)

Every member of staff has a responsibility to adhere to the Data Protection Principles outlined in the GDPR, and to this Data Protection Policy. Other relevant policies include the Social Media & Digital Comms Policy.

If you have a question about this Data Protection Policy or an area of concern about data protection matters, please contact our Data Protection Officer (DPO). The DPO is Director of Finance & Operations.

2. Data protection principles

There are six data protection principles defined in Article 5 of the GDPR. These require that all personal data be:

- processed in a **lawful**, **fair** and **transparent** manner.
- collected only for **specific**, **explicit** and **limited** purposes ('purpose limitation').
- **adequate**, **relevant** and **not excessive** ('data minimisation').
- **accurate** and kept **up-to-date** where necessary.
- kept for **no longer than necessary** ('retention').
- handled with appropriate **security** and **confidentiality**.

We are committed to upholding the data protection principles. All personal data under our control must be processed in accordance with these principles.

3. Lawful processing

3.1 All processing of personal data must meet one of the six lawful bases defined in Article 6(2) of the GDPR:

- Where we have the **consent** of the data subject

- Where it is in our **legitimate interests** and this is not overridden by the rights and freedoms of the data subject.
- Where necessary to meet a **legal obligation**.
- Where necessary to fulfil a **contract**, or pre-contractual obligations.
- Where we are protecting someone's **vital interests**.
- Where we are fulfilling a **public task,** or acting under official authority.

3.2 Any special category data (sensitive types of personal data as defined in Article 9(1) of the GDPR) must further be processed only in the line with one of the conditions specified in Article 9(2).

3.3 The most appropriate lawful basis will be noted in the Data Processing Register. (see 5. Accountability)

3.4 Where processing is based on consent, the data subject has the option to easily withdraw their consent.

3.5 Where electronic direct marketing communications are being sent, the recipient should have the option to opt-out in each communication sent, and this choice should be recognised and adhered to by us.

4. Data minimisation and control

4.1 Data collection processes will be regularly reviewed by the DPO to ensure that personal data collected and processed is kept to a minimum.

4.2 We will keep the personal data that we collect, use and share to the minimum amount required to be adequate for its purpose.

4.3 Where we do not have a legal obligation to retain some personal data, we will consider whether there is a business need to hold it.

4.4 We will retain personal data only for as long as it is necessary to meet its purpose. Our approach to retaining and erasing data no longer required will be specified in the retention policy and schedule. This schedule will be reviewed annually.

4.5 In the case of sharing personal data with any third party, only the data that is necessary to fulfil the purpose of sharing will be disclosed.

4.6 Anonymisation and pseudonymisation of personal data stored or transferred should be considered where doing so is a possibility.

5. Accountability

5.1 IRIS will maintain a Data Processing Register as required by Article 30 of the GDPR to document regular processing activities.

5.2 The 'Data Protection Officer' (DPO) has the specific responsibility of overseeing data protection and ensuring that we comply with the data protection principles and relevant legislation. (see 8. Role of the Data Protection Officer).

5.3 The DPO will ensure that the Data Processing Register is kept up to date and demonstrates how the data protection principles are adhered to by our activities. Individual members of staff have a duty to contribute to ensure that the measures outlined in the Register are accurately reflected in our practice.

5.4 The DPO monitors our compliance with relevant policies and regulatory requirements in respect of data protection.

5.5 All employees, consultants, partners or other parties who will be handling personal data on behalf of IRIS will be appropriately trained and supervised where necessary.

5.6 The collection, storage, use and sharing of personal data will be regularly reviewed by the Data Protection Officer.

5.7 We will adhere to relevant codes of conduct where they have been identified and discussed as appropriate.

5.8 Where there is likely to be a high risk to individuals rights and freedoms due to a processing activity, we will first undertake a Data Protection Impact Assessment (DPIA) and consult with the ICO prior to processing if necessary.

6. Use of processors

6.1 IRIS must only appoint processors who can provide sufficient guarantees around compliance with the GDPR and that the rights of data subjects will be protected.

6.2 Where a processor can demonstrate that they adhere to approved codes of conduct or certification schemes, this should be taken into consideration for choice of supplier.

6.3 Where IRIS uses a processor, a written contract with compulsory terms as set out in Article 28 of the GDPR must be in place (plus any additional requirements that we determine). Processors can only act on the instruction of IRIS.

7. Organisational Measures

7.1 All devices owned by IRIS will have hardware encryption set up by default where possible, including laptops, mobile devices and removable media.

7.2 All staff, contractors, temporary workers, consultants, partners or anyone else working on behalf of IRIS and handling personal data are bound by the data protection legislation and this Policy.

7.3 Where any contractor, temporary worker, consultant, or anyone else working on behalf of IRIS fails in their obligations under this Policy, they shall indemnify IRIS against any cost, liabilities, damages, loss, claims or proceedings that may arise from that failure.

8. Role of the Data Protection Officers

8.1 The Data Protection Officer role is assigned to a member of staff on a voluntary basis i.e. we are not legally obliged to have a DPO. We have chosen to do so as part of demonstrating our accountability and ensuring our compliance with data protection requirements.

8.2 The DPO assists IRIS to:

- monitor our internal compliance
- inform and advise on our data protection obligations
- provide advice regarding Data Protection Impact Assessments
- act as a contact point for data subjects and the Information Commissioner's Office.

8.3 The DPO advises and reports to Senior Management and to IRIS's Trustees on data protection matters.

8.4 The DPO is easily accessible as a point of contact for staff for data protection issues and is identified as the point of contact in our privacy notice and other external material.

8.5 The DPO identifies, organises and delivers training for staff and meets with new staff during their induction to discuss data protection matters, including this policy.

8.6 The DPO is required to have appropriate knowledge of data protection law and best practice, and is provided with adequate resources to help them carry out their role. This might include appropriate training and accreditation where identified.

8.7 The DPO is nominally responsible for carrying out responses to requests made by data subjects, reporting breaches and drawing up policies and procedures.

8.8 This does not preclude another responsible member of staff for carrying out these duties.

9. Rights of data subjects

9.1 Under data protection laws, data subjects have certain rights:

- **Right to be informed**. The right to be told how their personal data is used in clear and transparent language.
- **Right of access**. The right to know and have access to the personal data we hold about them.
- **Right to data portability**. The right to receive their data in a common and machine-readable electronic format.
- **Right to be forgotten**. The right to have their personal data erased.
- **Right to rectification**. The right to have their personal data corrected where it is inaccurate or incomplete.
- **Right to object**. The right to complain and to object to processing.
- **Right to purpose limitation**. The right to limit the extent of the processing of their personal data.
- **Rights related to automated decision-making and profiling**. The right not to be subject to decisions without human involvement.

10.1 We will uphold individuals' rights under data protection laws and allow them to exercise their rights over the personal data we hold about them. Privacy information will acknowledge these rights and explain how individuals can exercise them. Most rights are not absolute, and the individual will be able to exercise them depending on the circumstances, and exemptions may apply in some cases.

10.2 Any request in respect of these rights should be made in writing to **info@researchinschools.org**.

10.3 There is no fee for facilitating a request, unless it is 'manifestly unfounded or excessive', in which case administrative costs can be recovered.

10.4 Requests that are 'manifestly unfounded or excessive' can be refused.

10.5 We will take reasonable measures to require individuals to prove their identity where it is not obvious that they are the data subject.

10.6 We will respond to the request within one month from the date of request or being able to identify the person, unless it is particularly complex (in which case we will respond in no longer than 90 days).

10.7 The DPO will ensure that required actions are taken and that the appropriate response is facilitated within the deadline.

10.8 The DPO will draw up procedures for responding to requests where necessary, for example, for facilitating Subject Access Requests.

11. Reporting of breaches

11.1 A personal data breach means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data.

11.2 All members of staff should be vigilant and able to identify a suspected personal data breach. A breach could include:

- loss or theft of devices or data, including information stored on USB drives or on paper
- hacking or other forms of unauthorised access to a device, email account, or the network
- disclosing personal data to the wrong person, through wrongly addressed emails, or bulk emails that inappropriately reveal all recipients email addresses
- alteration or destruction of personal data without permission

11.3 Where a member of staff discovers or suspects a personal data breach, this should be reported to the DPO as soon as possible.

11.4 Where there is a likely risk to individuals' rights and freedoms, the DPO will report the personal data breach to the ICO within 72 hours of the organisation being aware of the breach.

11.5 Where there is also a likely high risk to individuals' rights and freedoms, IRIS will inform those individuals without undue delay.

11.6 The DPO will keep a record of all personal data breaches reported, and follow up with appropriate measures and improvements to reduce the risk of reoccurrence.