Bismilahir-Rahmanir-Rahim

IQRA SLOUGH ISLAMIC PRIMARY SCHOOL (ISIPS)

Data Protection/GDPR

We Learn, We Lead, We Inspire

Review Date..... 1st September 2026 ..

Approved by the Governing Body

Frequency of Review..... Annual .....

Next Review Date..... 1st September 2027 .....

Data Protection Policy

IQRA Primary School



Contents

1. Aims 3
2. Legislation and guidance 3
3. Definitions 4
4. The data controller 5
5. Roles and responsibilities 5
6. Data protection principles 6
7. Collecting personal data 6
8. Sharing personal data 7
9. Subject access requests and other rights of individuals 7
10. Parental requests to see the educational record 9
11. CCTV 9
12. Photographs and videos 9
13. Data protection by design and default 10
14. Data security and storage of records 10
15. Disposal of records 11
16. Personal data breaches 11
17. Training 11
18. Monitoring arrangements 11
19. Links with other policies 11
Appendix 1: Personal data breach procedure 12

1. Aims

Our school aims to ensure that all personal data collected about staff, pupils, parents, governors, visitors and other individuals is collected, stored and processed in accordance with the **General Data Protection Regulation (GDPR)**, the expected provisions of the **Data Protection Act 2018 (DPA 2018)** as set out in the Data Protection Bill and the Data Use and Access Act 2025.

This policy applies to all personal data, regardless of whether it is in paper or electronic format.

2. Legislation and guidance

This policy meets the requirements of the GDPR and the expected provisions of the DPA 2018 and the Data Use and Access Act 2025.

. It is based on guidance published by the Information Commissioner's Office (ICO) on the **GDPR** and the **ICO's code of practice for subject access requests**.

It meets the requirements of the Protection of Freedoms Act 2012 when referring to our use of biometric data.

It also reflects the ICO's code of practice for the use of surveillance cameras and personal information.

In addition, this policy complies with regulation 5 of the Education (Pupil Information) (England) Regulations 2005, which gives parents the right of access to their child's educational record.

3. Definitions

Term	Definition
Personal data	Any information relating to an identified, or identifiable, individual. This may include the individual's: • Name (including initials) • Identification number • Location data • Online identifier, such as a username It may also include factors specific to the individual's physical, physiological, genetic, mental, economic, cultural or social identity.
Special categories of personal data	Personal data which is more sensitive and so needs more protection, including information about an individual's: • Racial or ethnic origin • Political opinions • Religious or philosophical beliefs • Trade union membership • Genetics • Biometrics (such as fingerprints, retina and iris patterns), where used for identification purposes • Health – physical or mental • Sex life or sexual orientation
Processing	Anything done to personal data, such as collecting, recording, organising, structuring, storing, adapting, altering, retrieving, using, disseminating, erasing or destroying. Processing can be automated or manual.
Data subject	The identified or identifiable individual whose personal data is held or processed.
Data controller	A person or organisation that determines the purposes and the means of processing of personal data.
Data processor	A person or other body, other than an employee of the data controller, who processes personal data on behalf of the data controller.

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

4. The data controller

Our school processes personal data relating to parents, pupils, staff, governors, visitors and others, and therefore is a data controller.

The school is registered as a data controller with the ICO and will renew this registration annually or as otherwise legally required.

5. Roles and responsibilities

This policy applies to **all staff** employed by our school, and to external organisations or individuals working on our behalf. Staff who do not comply with this policy may face disciplinary action.

5.1 Governing board

The governing board has overall responsibility for ensuring that our school complies with all relevant data protection obligations.

5.2 Data protection officer

The data protection officer (DPO) is responsible for overseeing the implementation of this policy, monitoring our compliance with data protection law, and developing related policies and guidelines where applicable.

They will provide an annual report of their activities directly to the governing board and, where relevant, report to the board their advice and recommendations on school data protection issues.

The DPO is also the first point of contact for individuals whose data the school processes, and for the ICO.

Full details of the DPO's responsibilities are set out in their job description.

Our DPO is Spencer-West and is contactable via Iqra Primary School at dpo@iqra.slough.sch.uk

5.3 Headteacher

The headteacher acts as the representative of the data controller on a day-to-day basis.

5.4 All staff

Staff are responsible for:

- Collecting, storing and processing any personal data in accordance with this policy
- Informing the school of any changes to their personal data, such as a change of address
- Contacting the DPO in the following circumstances:
    - With any questions about the operation of this policy, data protection law, retaining personal data or keeping personal data secure
    - If they have any concerns that this policy is not being followed
    - If they are unsure whether or not they have a lawful basis to use personal data in a particular way
    - 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
    - If there has been a data breach
    - Whenever they are engaging in a new activity that may affect the privacy rights of individuals
    - If they need help with any contracts or sharing personal data with third parties

6. Data protection principles

The GDPR is based on data protection principles that our school must comply with.

The principles say that personal data must be:

- Processed lawfully, fairly and in a transparent manner
- Collected for specified, explicit and legitimate purposes
- Adequate, relevant and limited to what is necessary to fulfil the purposes for which it is processed
- Accurate and, where necessary, kept up to date
- Kept for no longer than is necessary for the purposes for which it is processed
- Processed in a way that ensures it is appropriately secure

This policy sets out how the school aims to comply with these principles.

7. Collecting personal data

7.1 What data we collect

We collect and store personal data to help support learning, monitor progress, and keep children safe. This may include:

- Names and contact details
- Date of birth
- Attendance records
- Medical information (e.g., allergies)
- Special educational needs
- Assessment and behaviour information
- Photographs and video (with permission)

7.2 Why We Collect Data

We collect data to:

- Support children's learning and development
- Keep children and staff safe
- Meet our legal duties (e.g., reporting to the Department for Education)
- Communicate with families
- Track progress and plan support

7.3 Lawfulness, fairness and transparency (covers the who we share data with)

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 the school 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 the school 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 the school, 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 the school 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 classroom apps, and we intend to rely on consent as a basis for processing, we will get parental consent (except for online counselling and preventive services).

7.2 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 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 the school's Information and Records Management Society's toolkit for schools.

8. Sharing personal data

We will not normally share personal data with anyone else, but may do so where:

- There is an issue with a pupil or parent/carer that puts the safety of our staff at risk
- We need to liaise with other agencies – we will seek consent as necessary before doing this
- Our suppliers or contractors need data to enable us to provide services to our staff and pupils – for example, IT companies. When doing this, we will:
    - Only appoint suppliers or contractors which can provide sufficient guarantees that they comply with data protection law
    - Establish a data sharing agreement with the supplier or contractor, either in the contract or as a standalone agreement, to ensure the fair and lawful processing of any personal data we share
    - Only share data that the supplier or contractor needs to carry out their service, and information necessary to keep them safe while working with us

We will also share personal data with law enforcement and government bodies where we are legally required to do so, including for:

- The prevention or detection of crime and/or fraud
- The apprehension or prosecution of offenders
- The assessment or collection of tax owed to HMRC
- In connection with legal proceedings
- Where the disclosure is required to satisfy our safeguarding obligations
- Research and statistical purposes, as long as personal data is sufficiently anonymised or consent has been provided

We may also share personal data with emergency services and local authorities to help them to respond to an emergency situation that affects any of our pupils or staff.

Where we transfer personal data to a country or territory outside the European Economic Area, we will do so in accordance with data protection law.

9. Subject access requests and other rights of individuals

9.1 Subject access requests

Individuals have a right to make a 'subject access request' to gain access to personal information that the school holds about them. This includes:

- Confirmation that their personal data is being processed

- Access to a copy of the data
- The purposes of the data processing
- The categories of personal data concerned
- Who the data has been, or will be, shared with
- How long the data will be stored for, or if this isn't possible, the criteria used to determine this period
- The source of the data, if not the individual
- Whether any automated decision-making is being applied to their data, and what the significance and consequences of this might be for the individual

Subject access requests should include:

- Name of individual
- Correspondence address
- Contact number and email address
- Details of the information requested

If staff receive a subject access request they must immediately forward it to the DPO.

9.2 Children and subject access requests

Personal data about a child belongs to that child, and not the child's parents or carers. For a parent or carer to make a subject access request with respect to their child, the child must either be unable to understand their rights and the implications of a subject access request, or have given their consent.

Children below the age of 12 are generally not regarded to be mature enough to understand their rights and the implications of a subject access request. Therefore, most subject access requests from parents or carers of pupils at our school may be granted without the express permission of the pupil. This is not a rule and a pupil's ability to understand their rights will always be judged on a case-by-case basis.

9.3 Responding to subject access requests

When responding to requests, we:

- May ask the individual to provide 2 forms of identification
- May contact the individual via phone to confirm the request was made
- Will respond without delay and within 1 month of receipt of the request
- Will provide the information free of charge
- May tell the individual we will comply within 3 months of receipt of the request, where a request is complex or numerous. We will inform the individual of this within 1 month, and explain why the extension is necessary

We will not disclose information if it:

- Might cause serious harm to the physical or mental health of the pupil or another individual
- Would reveal that the child is at risk of abuse, where the disclosure of that information would not be in the child's best interests
- Is contained in adoption or parental order records
- Is given to a court in proceedings concerning the child

If the request is unfounded or excessive, we may refuse to act on it, or charge a reasonable fee which takes into account administrative costs.

A request will be deemed to be unfounded or excessive if it is repetitive, or asks for further copies of the same information.

When we refuse a request, we will tell the individual why, and tell them they have the right to complain to the ICO.

9.4 Other data protection rights of the individual

In addition to the right to make a subject access request (see above), and to receive information when we are collecting their data about how we use and process it (see section 7), individuals also have the right to:

- Withdraw their consent to processing at any time
- Ask us to rectify, erase or restrict processing of their personal data, or object to the processing of it (in certain circumstances)
- Prevent use of their personal data for direct marketing
- Challenge processing which has been justified on the basis of public interest
- Request a copy of agreements under which their personal data is transferred outside of the European Economic Area
- Object to decisions based solely on automated decision making or profiling (decisions taken with no human involvement, that might negatively affect them)
- Prevent processing that is likely to cause damage or distress
- Be notified of a data breach in certain circumstances
- Make a complaint to the ICO
- Ask for their personal data to be transferred to a third party in a structured, commonly used and machine-readable format (in certain circumstances)

Individuals should submit any request to exercise these rights to the DPO. If staff receive such a request, they must immediately forward it to the DPO.

10. Parental requests to see the educational record

Parents, or those with parental responsibility, have a legal right to free access to their child's educational record (which includes most information about a pupil) within 15 school days of receipt of a written request.

11. CCTV

We use CCTV in various locations around the school site to ensure it remains safe. We will adhere to the ICO's code of practice for the use of CCTV.

We do not need to ask individuals' permission to use CCTV, but we make it clear where individuals are being recorded. Security cameras are clearly visible and accompanied by prominent signs explaining that CCTV is in use.

Any enquiries about the CCTV system should be directed to the Headteacher.

12. Photographs and videos

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

We will obtain written consent from parents/carers for photographs and videos to be taken of their child for communication, marketing and promotional materials. We will clearly explain how the photograph and/or video will be used to both the parent/carer and pupil.

Uses may include:

- Within school on notice boards and in school magazines, brochures, newsletters, etc.
- Outside of school by external agencies such as the school photographer, newspapers, campaigns
- Online on our school 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/Photographic and Video Images Policy for more information on our use of photographs and videos.

13. 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 (see section 6)
- Completing privacy impact assessments where the school's 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:
    - For the benefit of data subjects, making available the name and contact details of our school and DPO and all information we are required to share about how we use and process their personal data (via our privacy notices)
    - 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

14. 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
- Passwords that are at least 8 characters long containing letters and numbers are used to access school 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
- Staff, pupils or governors who store personal information on their personal devices are expected to follow the same security procedures as for school-owned equipment (see our E-Safety Policy/IT Policy)
- 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 (see section 8)

15. 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 school's behalf. If we do so, we will require the third party to provide sufficient guarantees that it complies with data protection law.

16. Personal data breaches

The school 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.

When appropriate, we will report the data breach to the ICO within 72 hours. Such breaches in a school context may include, but are not limited to:

- A non-anonymised dataset being published on the school website which shows the exam results of pupils eligible for the pupil premium
- Safeguarding information being made available to an unauthorised person
- The theft of a school laptop containing non-encrypted personal data about pupils

17. Training

All staff and governors 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.

18. 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 reviewed **every 2 years** and shared with the full governing board.

19. Links with other policies

This data protection policy is linked to our:

- Freedom of information policy
- Child Protection and Safeguarding Policy
- E-Safety Policy
- IT Usage Policy
- Computing Policy
- Photographic and Video Image Policy

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:
    - Lost
    - Stolen
    - Destroyed
    - Altered
    - Disclosed or made available where it should not have been
    - Made available to unauthorised people
- The DPO will alert the headteacher and the chair of governors
- 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:
    - Loss of control over their data
    - Discrimination
    - Identify theft or fraud
    - Financial loss
    - Unauthorised reversal of pseudonymisation (for example, key-coding)
    - Damage to reputation
    - Loss of confidentiality
    - 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.
- 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 school's computer system or in a locked filing cabinet in the Business Manager's office.
- 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:
    - 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:
    - 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 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:
    - Facts and cause
    - Effects
    - 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 school's computer system or in a locked filing cabinet in the Business Manager's office.

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

Actions to minimise the impact of data breaches

We will take appropriate actions 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.

Addendum Fair Processing Notice for Employees re: COVID-19

We are committed to protecting your personal data and being transparent about what data we process about you. This privacy notice applies to all employees, agency and other workers and it explains how we collect, use, process and share your personal data in relation to COVID-19 and your rights regarding your personal data.

We've used a Q&A method to explain:

- What information we collect about you;
- How we may use that information; and
- In what situations we may disclose your information to third parties.

1. Can we ask employees if they have any symptoms or to notify us if they have been diagnosed?

Yes. ICO states that it would be reasonable to ask people if they are experiencing symptoms.

Data about an employee's health, including whether or not they are experiencing COVID-19 symptoms, is "special category" personal data as defined in the GDPR.

As well as requiring a lawful basis for processing under Article 6, we need an additional exemption to process this data under Article 9.

The relevant legal bases are:

- compliance with health and safety obligations under employment law (GDPR Article 9(2)(b); DPA 2018 Sch.1 Para.1)
- for reasons of public health (GDPR Art.9(2)(i); DPA 2018 Sch.1 Para.3)

We will not be relying on your consent for the processing of your COVID-19 health data because consent from employees is generally not regarded as freely given (and is therefore invalid) due to the imbalance in power between the organisation and the individual. Therefore, relying on consent as the legal basis for processing is unlikely to be compliant with the GDPR.

We will:

- not collect more data than we need and we will limit the collection of your health data to COVID-19 only
- ensure collection of this data is in the least intrusive way possible
- make sure that we keep the data safe and secure and limit circulation on a 'need to know' basis only

2. Can we take employee's temperature readings?

Yes, if strictly necessary. ICO guidance does not prevent collecting and recording employees' temperatures.

Conducting health screening in an employment context needs to be carefully considered in the circumstances. It is only likely to be appropriate in a very small number of situations (e.g. where such testing is necessary to determine an employee's fitness to work, particularly when exposed to a risk group).

The available lawful bases are compliance with health and safety obligations under employment law (Article 9(2)(b) GDPR; para.1, Sch.1 DPA 2018) and for reasons of public health (Art.9(2)(i) GDPR; para.3, Sch.1 DPA 2018).

3. Can we ask about symptoms in the employee's household?

Yes. ICO states that, where necessary, the collection of additional data from employees may be proportionate. However, the data minimisation principle is key - do not collect more information than needed and ensure it is treated with appropriate safeguards. We will not collect information regarding specific symptoms about each household member.

4. Can we keep a record of staff who are diagnosed as infected?

Yes. Note that such collection of data would need to comply with data protection principles. In particular, data minimisation and purpose limitation will be important.

5. Can we notify other members of staff about an infected employee?

Yes. The ICO has advised that informing employees that a colleague may have contracted the virus is permitted by virtue of the employer's duty of care and to ensure the employees' health and safety.

Such information may, for example, facilitate contact tracing and thereby reduce virus exposure. However, this will be done on an anonymised and need-to-know basis, disclosing the minimum data required.

6. Can we notify customers and visitors of an infected employee?

Yes. We can notify our customers if an infected employee has interacted with customers or visitors.

It is unlikely that information about specific individuals will need to be disclosed. However, where identification is required, the processing of health-related personal data can be carried out under Art 9(2)(i) GDPR and para.3, Sch.1 DPA 2018, where it is necessary for reasons of public interest in the area of public health.

7. How long do we keep your COVID-19 health data?

We will hold your personal data for the duration of the pandemic and then as directed by the government.

8. Your rights in connection with your personal information

You have rights in respect of our processing of your personal data which are:

- To request access to your personal data and information about our processing of it. You also have the right to request a copy of your personal data (but we will need to remove information about other people).
- To request we rectify incorrect personal data that we are processing.
- To request that we erase your personal data if:
    - o we no longer need it;
    - o if we are processing your personal data by consent and you withdraw that consent;
    - o if we no longer have a legitimate ground to process your personal data; or
    - o we are processing your personal data unlawfully
- To object to our processing if it is by legitimate interest.
- To restrict our processing if it was by legitimate interest.
- To request that your personal data be transferred from us to another company if we were processing your data under a contract or with your consent and the processing is carried out automated means.

If you want to exercise any of these rights, please contact us.
If you have any questions or concerns, please contact us as most matters can be resolved informally in the first instance.

You also have the right to lodge a complaint about our processing via the UK's Information Commissioner's Office.

Data Protection Complaints Procedure

1. Purpose

This procedure explains how IQRA Primary School receives, records, investigates and responds to complaints about the way it handles personal data.

It is intended to ensure that data protection complaints are handled fairly, promptly, consistently and transparently, and in a way that demonstrates accountability under UK data protection law.

This procedure is designed to reflect the requirements introduced by section 103 of the Data (Use and Access) Act 2025, which inserts a new section 164A into the Data Protection Act 2018.

2. Scope

This procedure applies to all complaints about the processing of personal data by IQRA Primary School. It applies to complaints made by customers, clients, employees, workers, former employees, contractors, service users, suppliers, website users, patients or beneficiaries and any other individual whose personal data is processed by IQRA Primary School.

It applies whether a complaint is received by email, post, webform, telephone, live chat, social media, in person, through a service team or through any other channel.

3. What counts as a data protection complaint?

A data protection complaint is any complaint from an individual, or someone acting on their behalf, about how IQRA Primary School has handled that individual's personal data. The individual does not need to refer to the UK GDPR, the Data Protection Act, the Data Use and Access Act or the phrase 'data protection complaint'. Staff must look at the substance of the concern.

how personal data was collected or obtained;
how personal data has been used, shared or disclosed;
inaccurate, incomplete or out-of-date personal data;
personal data being kept for too long;
a data breach or suspected security incident;
a delayed, incomplete or disputed subject access response;
a refusal or failure to deal with a request for erasure, rectification, restriction, portability or objection;
direct marketing, cookies or tracking technologies;
automated decision-making or profiling;
failure to provide clear privacy information.

4. Responsibility

Role	Responsibility
Procedure owner	DPO@iqra.slough.sch.uk / Data Protection Lead
Operational owner	Front Office Team / Data Protection Lead
Senior escalation	Head Teacher / SLT / Governors
All staff	Must recognise potential data protection complaints and escalate them promptly.

The Data Protection Lead is responsible for maintaining this procedure, overseeing data protection complaints, ensuring complaints are logged, advising on investigations, ensuring appropriate responses are provided, identifying themes and escalating significant issues.

5. How individuals can make a complaint

IQRA Primary School will facilitate the making of data protection complaints through accessible routes. Individuals can complain using any of the following methods:

Route	Details
Email	DPO@iqra.slough.sch.uk
Post	Fernside, Off Wexham Road, Slough, Berks. SL2 5FF
Telephone	01753 520018
In person	To any member of staff, who must escalate the matter internally.
Other channels	Complaints received through service teams, customer portals, HR, social media or general inboxes must still be accepted and escalated.

Individuals should be asked to provide their name, contact details, details of the complaint, the personal data concerned, relevant dates, copies of relevant correspondence, and the outcome they are seeking. However, IQRA Primary School will not refuse to consider a complaint simply because the individual has not used a particular form or has not provided all information at the outset.

6. Complaints made on behalf of another person

A complaint may be made by someone acting on behalf of an individual, such as a family member, solicitor, advocate, representative, person with power of attorney, parent or guardian.

Before disclosing personal data to a representative, IQRA Primary School must be satisfied that the representative has authority to act. Suitable evidence may include written authority from the individual, a signed consent form, power of attorney documentation, evidence of parental responsibility or evidence that the representative is otherwise legally entitled to act.

Authority checks must not be used to delay or obstruct a complaint. The complaint must be logged on receipt while any authority checks are completed.

7. Receiving and identifying complaints

Any member of staff who receives a complaint that may involve personal data must forward it to the Data Protection Lead as soon as possible and, in any event, within two working days.

Staff must not decide whether the complaint is legally valid before escalating it. If the substance of the concern relates to personal data, it must be escalated.

Where a complaint includes both a service complaint and a data protection complaint, the data protection element must be handled under this procedure. The wider service complaint may be handled under IQRA Primary School's general complaints process.

8. Logging the complaint

All data protection complaints must be recorded in the Data Protection Complaints Log. The log should be maintained by the Data Protection Lead or nominated complaints team.

Log field	What to record
Complaint reference	Unique complaint number.
Date received	Date the complaint was first received by IQRA Primary School.
Method received	Email, post, webform, telephone, in person, social media or other.
Complainant details	Name and contact details.
Representative	Whether the complaint is made by a representative and whether authority has been checked.
Summary	Brief description of the complaint and the personal data issue.

Category	Subject access, erasure, accuracy, breach, sharing, marketing, retention or other.
Business area	Team, service or function involved.
Investigator	Responsible person or team.
Acknowledgement deadline	30-day deadline calculated from receipt.
Updates and outcome	Progress updates, outcome date and decision.
Remedial action	Action required, owner and completion date.
ICO escalation	Whether the complainant has complained to the ICO.
Lessons learned	Any wider action required.

9. Acknowledging the complaint

IQRA Primary School will acknowledge receipt of a data protection complaint within 30 days of receiving it. The 30-day period starts on the day after the complaint is received. If the final day falls on a weekend or public holiday, acknowledgement can be sent on the next working day.

The acknowledgement should confirm that the complaint has been received, explain that it is being handled as a data protection complaint, provide the complaint reference number, identify the person or team handling the complaint, explain whether any further information is needed, explain the next steps, and provide an indicative timescale for a response where possible.

10. Investigation

The investigation must begin without undue delay. IQRA Primary School should not wait until the end of the 30-day acknowledgement period before starting to investigate.

The investigator should consider:

what personal data is involved;
what processing activity is being complained about;
whether the complaint relates to a rights request;
whether a personal data breach may have occurred;
whether a processor, supplier or joint controller is involved;
whether [IQRA Primary School] complied with the UK GDPR, Data Protection Act 2018 and internal policies;
whether remedial action is required;
whether the complaint raises wider organisational risks.
Investigation steps may include reviewing correspondence, checking systems and records, speaking to relevant staff, reviewing access logs or audit trails, checking privacy notices and policies, reviewing contracts or processor arrangements, checking whether a DPIA or legitimate interests assessment is relevant and obtaining legal or specialist advice where appropriate.

11. Keeping the complainant informed

Where a complaint cannot be resolved quickly, IQRA Primary School will keep the complainant informed about progress.

Updates should be provided where the complaint is complex, further information is needed, the investigation is taking longer than expected, third-party input is required, or IQRA Primary School needs more time to reach a fair outcome.

Updates must be clear, brief and meaningful. They must not disclose information about other individuals unless it is lawful and appropriate to do so.

12. Outcome response

Once the investigation is complete, IQRA Primary School will provide the complainant with an outcome without undue delay.

The outcome response should include:

a summary of the complaint;
the issues investigated;
IQRA Primary School's findings;
whether the complaint is upheld, partially upheld or not upheld;
reasons for the decision;
any action already taken;
any further action IQRA Primary School will take;
any apology, where appropriate;
details of the complainant's right to complain to the ICO.

13. Possible outcomes

Outcome	Meaning
Upheld	IQRA Primary School accepts that the complaint is justified in full.
Partially upheld	IQRA Primary School accepts some elements of the complaint but not all.
Not upheld	IQRA Primary School does not accept that there has been a failure, and explains why.
Corrective action	This may include correction, erasure, restriction, process change, training, supplier review, security improvement or further response to an individual rights request.
No further action	Where no further action is required, IQRA Primary School should still explain the reasons clearly.

14. Escalation

The Data Protection Lead must escalate a complaint to senior management/DPO where:

the complaint involves a serious or repeated data protection issue;
there is a risk of significant harm to an individual;
the complaint relates to special category data or criminal offence data;
the complaint relates to a vulnerable individual;
the complaint concerns a senior employee or high-risk processing activity;
the complaint may result in litigation;
the complaint may be reported to the ICO;
the complaint may create reputational risk;
a personal data breach may have occurred.
Where the complaint suggests that a personal data breach may have occurred, IQRA Primary School's personal data breach procedure must also be followed.

15. Complaints involving processors, suppliers or joint controllers

Where a complaint involves a processor, supplier or joint controller, the Data Protection Lead must identify the relevant contract, data processing agreement or data sharing arrangement.

IQRA Primary School should consider whether the third party needs to assist with the investigation, whether it has complied with contractual obligations, whether personal data has been processed outside agreed instructions, whether breach notification obligations have been triggered and whether remedial action is required.

Processors must be required to escalate data protection complaints to IQRA Primary School promptly where the complaint relates to personal data processed on behalf of IQRA Primary School.

16. Complaints involving individual rights requests

Where a complaint concerns a subject access request or other individual rights request, the Data Protection Lead must review the original request, the response provided, the timeframe for response, any exemptions relied upon, searches carried out, redactions applied, information withheld, and correspondence with the individual.

If the complaint identifies an error or omission, IQRA Primary School should correct it promptly.

17. Interaction with the ICO

Individuals have the right to complain to the Information Commissioner's Office if they are dissatisfied with how their personal data has been handled.

Outcome responses should include the ICO's contact details:

ICO contact	Detail
Website	www.ico.org.uk
Telephone	0303 123 1113

18. Record keeping

IQRA Primary School must retain appropriate records of data protection complaints and how they were handled. Records should include the complaint received, acknowledgement sent, internal investigation notes, evidence reviewed, internal decisions, correspondence with the complainant, outcome response, remedial actions and closure date.

Complaint records should be retained for six years from closure unless a longer period is required due to litigation, regulatory investigation, safeguarding, insurance or other legal reasons. If a longer period is required, this must be noted on the register along with the reasons why.

19. Confidentiality

Data protection complaints must be handled confidentially. Information about a complaint should only be shared with staff or third parties who need access in order to investigate, respond, take advice or implement remedial action.

IQRA Primary School must avoid disclosing personal data about other individuals unless it is lawful and necessary to do so.

20. Monitoring and reporting

The Data Protection Lead will review the Data Protection Complaints Log at least quarterly. The review should consider the number of complaints received, categories, response times, overdue complaints, repeat issues, business areas involved, upheld or partially upheld complaints, ICO escalations, remedial actions, training needs and process improvements.

A summary report should be provided to Head Teacher / Governors at least annually.

21. Staff training

All staff must receive appropriate training so that they can recognise and escalate data protection complaints. Training should cover what a data protection complaint is, how complaints may be received, why legal terminology is not required, who complaints should be escalated to, the importance of prompt escalation, confidentiality, the 30-day acknowledgement requirement and the need to avoid deleting or altering relevant records.

22. Review of this procedure

This procedure will be reviewed annually, following changes to data protection law or ICO guidance, following a serious complaint, following an ICO complaint or investigation or where monitoring identifies recurring issues.

21. Staff training

All staff must receive appropriate training so that they can recognise and escalate data protection complaints. Training should cover what a data protection complaint is, how complaints may be received, why legal terminology is not required, who complaints should be escalated to, the importance of prompt escalation, confidentiality, the 30-day acknowledgement requirement and the need to avoid deleting or altering relevant records.

22. Review of this procedure

This procedure will be reviewed annually, following changes to data protection law or ICO guidance, following a serious complaint, following an ICO complaint or investigation or where monitoring identifies recurring issues.

Appendix 1: Data protection complaint acknowledgement template

Subject: Your data protection complaint

Dear [Name],

Thank you for contacting us.

We acknowledge receipt of your complaint dated [date] about [brief description]. We are treating this as a data protection complaint.

Your complaint reference is: [reference number].

We will review the matters you have raised and may contact you if we need any further information. We will keep you informed about the progress of our investigation and will provide an outcome without undue delay.

If you have any questions in the meantime, please contact [name/team] at [email address].

Yours sincerely,

[Name]

[Role]

Appendix 2: Data protection complaint outcome template

Subject: Outcome of your data protection complaint

Dear [Name],

We are writing further to your data protection complaint dated [date].

Summary of your complaint: You complained that [summary of complaint].

What we considered: As part of our investigation, we reviewed [records reviewed], [systems checked], [staff or teams consulted] and [policies or procedures reviewed].

Our findings: We have found that [set out findings clearly]. Your complaint is [upheld / partially upheld / not upheld]. The reasons for our decision are [insert reasons].

Action taken: We have taken, or will take, the following action: [insert action].

Right to complain to the ICO: If you are unhappy with our response, you have the right to complain to the Information Commissioner's Office. You can contact the ICO through its website at www.ico.org.uk or by telephone on 0303 123 1113.

Yours sincerely,

[Name]

[Role]

Appendix 3: Data protection complaints log

Field	Details
Complaint reference	Unique complaint number.
Date received	Date the complaint was first received by IQRA Primary School
Method received	Email, post, webform, telephone, in person, social media or other.
Complainant details	Name and contact details.
Representative	Whether the complaint is made by a representative and whether authority has been checked.
Summary	Brief description of the complaint and the personal data issue.
Category	Subject access, erasure, accuracy, breach, sharing, marketing, retention or other.
Business area	Team, service or function involved.
Investigator	Responsible person or team.
Acknowledgement deadline	30-day deadline calculated from receipt.
Updates and outcome	Progress updates, outcome date and decision.
Remedial action	Action required, owner and completion date.
ICO escalation	Whether the complainant has complained to the ICO.
Lessons learned	Any wider action required.
Closure date	Date the complaint was closed.
Review date	Date any lessons learned or action plan was reviewed.