Rochdale Islamic Academy
inspire - believe - achieve
GIRLS' SCHOOL

GENERAL DATA PROTECTION POLICY (GDPR) P.29.

Reviewed: January 2020
Next Review: July 2021
Responsible: Mehnaz Kauser

Governing Body Approved: September 2020
Approved: Mr Javaid Kashif (Chair of Governors)

General Data Protection Regulations

Table of Contents

1. Our Commitment

Rochdale Islamic Academy is required to keep and process certain information about its staff members, pupils and parents in accordance with its legal obligations under the General Data Protection Regulation (GDPR). The school may, from time to time, be required to share personal information about its staff or pupils with other organisations, mainly the LA, Department for Education, other schools and educational bodies, children's services and other third parties, such as payroll providers or cashless till services. Rochdale Islamic Academy is committed to the protection of all personal and sensitive data for which it holds responsibility as the Data Controller and of the handling of such data in line with the data protection principles and the Data Protection Act (DPA)

This policy is in place to ensure all staff and governors are aware of their responsibilities and outlines how the school complies with the following core principles of the GDPR.

Organisational methods for keeping data secure are imperative, and Rochdale Islamic Academy believes that it is good practice to keep clear practical policies, backed up by written procedures.

This policy complies with the requirements set out in the GDPR, which will come into effect on 25 May 2018. The government have confirmed that the UK's decision to leave the EU will not affect the commencement of the GDPR.

Legal Framework

This policy has due regard to legislation, including, but not limited to the following:

- The General Data Protection Regulation (GDPR)
- The Freedom of Information Act 2000 ☐ The Education (Pupil Information) (England) Regulations
- The Education (Pupil Information) (England) Regulations 2005 (as amended in 2016) ☐ The Freedom of Information and Data Protection (Appropriate Limit and Fees) Regulations 2004 ☐ The School Standards and Framework Act 1998

This policy will also have regard to the following guidance:

- Information Commissioner's Office (2017) 'Overview of the General Data Protection Regulation (GDPR)'
- Information Commissioner's Office (2017) 'Preparing for the General Data Protection Regulation (GDPR) 12 steps to take now'

Accountability

Rochdale Islamic Academy will implement appropriate technical and organisational measures to demonstrate that data is processed in line with the principles set out in the GDPR.

The school will provide comprehensive, clear and transparent privacy policies.

Records of activities relating to higher risk processing will be maintained, such as the processing of special categories data or that in relation to criminal convictions and offences.

2. Notification

Our data processing activities will be registered with the Information Commissioner's Office (ICO) as required of a recognised Data Controller. Details are available from the ICO: https://ico.org.uk/about-the-ico/what-we-do/register-of-data-controllers/

Changes to the type of data processing activities being undertaken shall be notified to the ICO and details amended in the register.

Breaches of personal or sensitive data shall be notified within 72 hours to the individual(s) concerned and the ICO.

Data Protection Officer (DPO)

A DPO will be appointed in order to:

- Inform and advise the school and its employees about their obligations to comply with the GDPR and other data protection laws.
- Monitor the school's compliance with the GDPR and other laws, including managing internal data protection activities, advising on data protection impact assessments, conducting internal audits, and providing the required training to staff members.

An existing employee can be appointed to the role of DPO provided that their duties are compatible with the duties of the DPO and do not lead to a conflict of interests.

The individual appointed as DPO will have training and knowledge of data protection law, particularly that in relation to schools.

The DPO will report to the highest level of management at the school, which is the Head Teacher.

The DPO will operate independently and will not be dismissed or penalised for performing their task.

Sufficient resources will be provided to the DPO to enable them to meet their GDPR obligations.
Lawful

Lawful Processing

The legal basis for processing data will be identified and documented prior to data being processed. Under the GDPR, data will be lawfully processed under the following conditions:

- The consent of the data subject has been obtained.
- Processing is necessary for:

— Compliance with a legal obligation.
— The performance of a task carried out in the public interest or in the exercise of official authority vested in the controller.
— For the performance of a contract with the data subject or to take steps to enter into a contract.
— Protecting the vital interests of a data subject or another person.
— For the purposes of legitimate interests pursued by the controller or a third party, except where such

interests are overridden by the interests, rights or freedoms of the data subject. (This condition is not available to processing undertaken by the school in the performance of its tasks.)

Sensitive data will only be processed under the following conditions:

- Explicit consent of the data subject, unless reliance on consent is prohibited by EU or Member State law.
- Processing carried out by a not-for-profit body with a political, philosophical, religious or trade union aim provided the processing relates only to members or former members (or those who have regular contact with it in connection with those purposes) and provided there is no disclosure to a third party without consent.
- Processing relates to personal data manifestly made public by the data subject.
- Processing is necessary for:
  — Carrying out obligations under employment, social security or social protection law, or a collective agreement.
  — Protecting the vital interests of a data subject or another individual where the data subject is physically or legally incapable of giving consent.
  — The establishment, exercise or defence of legal claims or where courts are acting in their judicial capacity.

Consent

- Consent must be a positive indication. It cannot be inferred from silence, inactivity or pre-ticked boxes.
- Consent will only be accepted where it is freely given, specific, informed and an unambiguous indication of the individual's wishes.
- Where consent is given, a record will be kept documenting how and when consent was given.
- The school ensures that consent mechanisms meet the standards of the GDPR. Where the standard of consent cannot be met, an alternative legal basis for processing the data must be found, or the processing must cease.
- Consent accepted under the DPA will be reviewed to ensure it meets the standards of the GDPR; however, acceptable consent obtained under the DPA will not be re-obtained.
- Consent can be withdrawn by the individual at any time.
- Where a child is under the age of 16 or younger if the law provides it (up to the age of 13), the consent of parents will be sought prior to the processing of their data, except where the processing is related to preventative or counselling services offered directly to a child.

The Right of Access

Individuals have the right to obtain confirmation that their data is being processed.
Individuals have the right to submit a Subject Access Request (SAR) to gain access to their personal data in order to verify the lawfulness of the processing.

The school will verify the identity of the person making the request before any information is supplied.

A copy of the information will be supplied to the individual free of charge; however, the school may impose a 'reasonable fee' to comply with requests for further copies of the same information.

Where a SAR has been made electronically, the information will be provided in a commonly used electronic format.

Where a request is manifestly unfounded, excessive or repetitive, a reasonable fee will be charged.

All fees will be based on the administrative cost of providing the information.

All requests will be responded to without delay and at the latest, within one month of receipt.
In the event of numerous or complex requests, the period of compliance will be extended by a further two months. The individual will be informed of this extension, and will receive an explanation of why the extension is necessary, within one month of the receipt of the request.

Where a request is manifestly unfounded or excessive, the school holds the right to refuse to respond to the request. The individual will be informed of this decision and the reasoning behind it, as well as their right to complain to the supervisory authority and to a judicial remedy, within one month of the refusal.

In the event that a large quantity of information is being processed about an individual, the school will ask the individual to specify the information the request is in relation to.

The Right to Rectification

Individuals are entitled to have any inaccurate or incomplete personal data rectified.
Where the personal data in question has been disclosed to third parties, the school will inform them of the rectification where possible.

Where appropriate, the school will inform the individual about the third parties that the data has been disclosed to.

Requests for rectification will be responded to within one month; this will be extended by two months where the request for rectification is complex.

Where no action is being taken in response to a request for rectification, the school will explain the reason for this to the individual, and will inform them of their right to complain to the supervisory authority and to a judicial remedy.

The Right to Erasure

Individuals hold the right to request the deletion or removal of personal data where there is no compelling reason for its continued processing.

Individuals have the right to erasure in the following circumstances:

- Where the personal data is no longer necessary in relation to the purpose for which it was originally collected/processed
- When the individual withdraws their consent
- When the individual objects to the processing and there is no overriding legitimate interest for continuing the processing
- The personal data was unlawfully processed
- The personal data is required to be erased in order to comply with a legal obligation
- The personal data is processed in relation to the offer of information society services to a child

The school has the right to refuse a request for erasure where the personal data is being processed for the following reasons:

- 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
- The exercise or defence of legal claims

As a child may not fully understand the risks involved in the processing of data when consent is obtained, special attention will be given to existing situations where a child has given consent to processing and they later request erasure of the data, regardless of age at the time of the request.

Where personal data has been disclosed to third parties, they will be informed about the erasure of the personal data, unless it is impossible or involves disproportionate effort to do so.

Where personal data has been made public within an online environment, the school will inform other organisations who process the personal data to erase links to and copies of the personal data in question.

3. Personal and Sensitive Data

All data within the school's control shall be identified as personal, sensitive or both to ensure that it is handled in compliance with legal requirements and access to it does not breach the rights of the individuals to whom it relates.

The definitions of personal and sensitive data shall be as those published by the ICO for guidance: https://ico.org.uk/for-organisations/guide-to-data-protection/key- definitions/

The principles of the Data Protection Act shall be applied to all data processed:

- ensure that data is fairly and lawfully processed
- process data only for limited purposes
- ensure that all data processed is adequate, relevant and not excessive
- ensure that data processed is accurate
- not keep data longer than is necessary
- process the data in accordance with the data subject's rights
- ensure that data is secure
- ensure that data is not transferred to other countries without adequate protection.

4. Fair Processing / Privacy Notice

We shall be transparent about the intended processing of data and communicate these intentions via notification to staff, parents and pupils prior to the processing of individual's data.

Notifications shall be in accordance with ICO guidance and, where relevant, be written in a form understandable by those defined as 'Children' under the legislation.
https://ico.org.uk/for-organisations/guide-to-data-protection/privacy-notices- transparency-and-control/

There may be circumstances where the school is required either by law or in the best interests of our students or staff to pass information onto external authorities, for example Local Authorities, Department for Education, Exam Boards, Ofsted, or the Department of Health. These authorities are up to date with data protection law and have their own policies relating to the protection of any data that they receive or collect.

The intention to share data relating to individuals to an organisation outside of our school shall be clearly defined within notifications and details of the basis for sharing given. Data will be shared with external parties in circumstances where it is a legal requirement to provide such information.

Any proposed change to the processing of individual's data shall first be notified to them.

Under no circumstances will the school disclose information or data:

- that would cause serious harm to the child or anyone else's physical or
- mental health or condition
- indicating that the child is or has been subject to child abuse or may be at
- risk of it, where the disclosure would not be in the best interests of the child
- recorded by the pupil in an examination
- that would allow another person to be identified or identifies another
- person as the source, unless the person is an employee of the school or a local authority or has given consent, or it is reasonable in the circumstances to disclose the information without consent. The exemption from disclosure does not apply if the information can be edited so that the person's name or identifying details are removed
- in the form of a reference given to another school or any other place of
- education and training, the child's potential employer, or any national body concerned with student admissions.

5. Data Security

6. Data Access Requests (Subject Access Requests)

All individuals whose data is held by us, has a legal right to request access to such data or information about what is held. We shall respond to such requests within one month and they should be made in writing to:

(Name of senor person responsible for GDPR)
(Designation)
(Address/Contact of School)

No charge will be applied to process the request.

Personal data about pupils will not be disclosed to third parties without the consent of the child's parent or carer, unless it is obliged by law or in the best interest of the child.

Data may be disclosed to the following third parties without consent:

- **Other schools**

If a pupil transfers from (Name of School) to another school, their academic records and other data that relates to their health and welfare will be forwarded onto the new school. This will support a

smooth transition from one school to the next and ensure that the child is provided for as is necessary. It will aid continuation which should ensure that there is minimal impact on the child's academic progress as a result of the move.

- **Examination Boards/NFER**

This may be for registration purposes, to allow the pupils at our school to sit examinations set by external exam bodies.

- **Health authorities**

As obliged under health legislation, the school may pass on information regarding the health of children in the school to monitor and avoid the spread of contagious diseases in the interest of public health.

- **Police and courts**

If a situation arises where a criminal investigation is being carried out we may have to forward information on to the police to aid their investigation. We will pass information onto courts as and when it is ordered.

- **Social workers and support agencies**

In order to protect or maintain the welfare of our pupils, and in cases of child abuse, it may be necessary to pass personal data on to social workers or support agencies.

- **Educational division**

Schools may be required to pass data on in order to help the government to monitor the national educational system and enforce laws relating to education.

7. Photographs and Video

8. Location of information and data:

Hard copy data, records, and personal information are stored out of sight and in a locked cupboard. The only exception to this is medical information that may require immediate access during the school day. This will be stored with the school medical coordinator.

Sensitive or personal information and data should not be removed from the school site, however the school acknowledges that some staff may need to transport data between the school and their home in order to access it for work in the evenings and at weekends. This may also apply in cases where staff have offsite meetings, or are on school visits with pupils.

9. Guidelines for Staff

The following guidelines are in place for staff in order to reduce the risk of personal data being compromised:

- Paper copies of data or personal information should not be taken off the school site. If these are misplaced they are easily accessed. If there is no way to avoid taking a paper copy of data off the school site, the information should not be on view in public places, or left unattended under any circumstances.
- Unwanted paper copies of data, sensitive information or pupil files should be shredded. This also applies to handwritten notes if the notes reference any other staff member or pupil by name.

- Care must be taken to ensure that printouts of any personal or sensitive information are not left in printer trays or photocopiers.
- If information is being viewed on a PC, staff must ensure that the window and documents are properly shut down before leaving the computer unattended. Sensitive information should not be viewed on public computers.
- If it is necessary to transport data away from the school, it should be downloaded onto a USB stick. The data should not be transferred from this stick onto any home or public computers. Work should be edited from the USB, and saved onto the USB only.
- USB sticks that staff use must be password protected.

These guidelines are clearly communicated to all school staff, and any person who is found to be intentionally breaching this conduct will be disciplined in line with the seriousness of their misconduct.

Data Security

Confidential paper records will be kept in a locked filing cabinet, drawer or safe, with restricted access.
Confidential paper records will not be left unattended or in clear view anywhere with general access.
Digital data both on a local hard drive and on the school's network is password-protected. The network drive is backed up daily off-site.
Access to the school's network is controlled and access to sensitive and confidential data on the network is restricted to only those members of staff who require the information to perform their duties effectively.
Access to the school's management information system SIMS is password-protected and access to sensitive and confidential data on SIMS is restricted to only those members of staff who require the information to perform their duties effectively.
Staff are not permitted to use removable storage e.g. external hard drives or memory sticks to store data.
All electronic devices are password-protected to protect the information on the device in case of theft. Electronic devices are kept securely when not in use, e.g. in a locked cabinet.
Devices holding pupil and staff photos will be regularly wiped to delete all images. Memory cards will be kept in a locked cabinet when not in use and will be wiped regularly.

Access to all Office computers and Tapestry Online Learning Journal is password protected. When a member of staff leaves the company these passwords are changed in line with this policy and our Safeguarding policy. Any portable data storage used to store personal data, e.g. USB memory stick, are password protected and/or stored in a locked filing cabinet.
GDPR means that Rainbow Pre-school Southampton Limited must; * Manage and process personal data properly * Protect the individual's rights to privacy * Provide an individual with access to all personal information held on them

Where possible, the school enables electronic devices to allow the remote blocking or deletion of data in case of theft.
Staff, governors and student teachers, will not use their personal laptops or computers for school purposes.
All necessary members of staff are provided with their own secure login and password, and every computer regularly prompts users to change their password.

Staff, governors and student teachers must not use personal email addresses for sharing or viewing any school data. Secure LGFL email accounts are provided for all staff and governors.
Emails containing sensitive or confidential information are password-protected if there are unsecure servers between the sender and the recipient.
Circular emails to parents are sent blind carbon copy (bcc), so email addresses are not disclosed to other recipients.
When sending confidential information by fax, staff will always check that the recipient is correct before sending.
No personal data or sensitive personal data must be shared by text or on social media e.g. Whatsapp. See also the school's e-Safety and IT Acceptable Use Policy.
Where personal information that could be considered private or confidential is taken off the premises, either in electronic or paper format, staff will take extra care to follow the same procedures for security, e.g. keeping devices or paperwork under lock and key. The person taking the information from the school premises accepts full responsibility for the security of the data.
Before sharing data, all staff members will ensure:
☐ They are allowed to share it. ☐ That adequate security is in place to protect it. ☐ The person or organisation who will receive the data has been outlined in a privacy notice. ☐ The person or organisation who will receive the data have confirmed in writing that they comply with the GDPR and any other relevant data protection legislation. Under no circumstances are volunteers, visitors or unauthorised third parties allowed access to confidential or personal information. Those visiting areas of the school containing sensitive information are supervised at all times.
The physical security of the school's buildings and storage systems, and access to them, is reviewed on a regular basis. If an increased risk in vandalism/burglary/theft is identified, extra measures to secure data storage will be put in place.
Elmwood Infant School takes its duties under the GDPR seriously and any unauthorised disclosure may result in disciplinary action.
The Office Manager is responsible for continuity and recovery measures are in place to ensure the security of protected data.

Data Breaches
The term 'personal data breach' refers to a breach of security which has led to the destruction, loss, alteration, unauthorised disclosure of, or access to, personal data.
The Head Teacher will ensure that all staff members are made aware of, and understand, what constitutes a data breach as part of their CPD training.
Staff must report any data breach or potential breach as soon as possible to the Data Protection Officer or a member of the Senior Management Team.
Where a breach is likely to result in a risk to the rights and freedoms of individuals, the relevant supervisory authority will be informed.

CCTV and Photography
The school understands that recording images of identifiable individuals constitutes processing personal information, so it is done in line with data protection principles.

Cameras are only placed where they do not intrude on anyone's privacy and are necessary to fulfil their purpose.

All CCTV footage will be kept for 30 days for security purposes; the Office Manager is responsible for keeping the records secure and allowing access.

The school will always indicate its intentions for taking photographs of pupils and will obtain permission before publishing them.

If the school wishes to use images/video footage of pupils in a publication, such as the school website, prospectus, or recordings of school plays, written permission will be sought for the particular usage from the parent of the pupil.

Images captured by individuals for recreational/personal purposes, and videos made by parents for family use, are exempt from the GDPR.

Data Retention and Storing Pupil Data

Data will not be kept for longer than is necessary. The school follows the Information Commissioner's guidance on retention of documents, including the Information and records Management Society's Retention Guidelines for School.
Unrequired data will be deleted as soon as practicable.

Some educational records relating to former pupils or employees of the school may be kept for an extended period for legal reasons.

Paper documents will be shredded or pulped, and electronic memories scrubbed clean or destroyed, once the data should no longer be retained.

DBS Data
All data provided by the DBS will be handled in line with data protection legislation; this includes electronic communication.

Data provided by the DBS will never be duplicated.
Any third parties who access DBS information will be made aware of the data protection legislation, as well.

10. Data Disposal

The school recognises that the secure disposal of redundant data is an integral element to compliance with legal requirements and an area of increased risk.

All data held in any form of media (paper, tape, electronic) shall only be passed to a disposal partner with demonstrable competence in providing secure disposal services.

11. Appendices

Appendices 2
Privacy Impact Assessment

What is the aim of the activity?
What data will be collected?

How will the data be collected?
Where will the data be stored
How will the data be shared
How will the data be amended or deleted
Identified risks that include issues, risks to individuals, compliance risks, school risk and possible solutions

Privacy Impact Statement prepared by:	Date:

Appendices 3

Subject Access Request Form

You should complete this form if you want us to supply you with a copy of any personal data we hold about you. You are currently entitled to receive this information under the Data Protection Act 1998 (DPA) and will continue to be under the EU General Data Protection Regulation (GDPR), which comes into effect on 25 May 2018.

We will also provide you with information about any processing of your personal data that is being carried out, the retention periods which apply to your personal data, and any rights to rectification, erasure, or restriction of processing that may exist.

We will endeavour to respond promptly and in any event within one month of the latest of the following:

Our receipt of your written request; or

Our receipt of any further information we may ask you to provide to enable us to comply with your request.

The information you supply in this form will only be used for the purposes of identifying the personal data you are requesting and responding to your request. You are not obliged to complete this form to make a request, but doing so will make it easier for us to process your request quickly.

SECTION 1: Details of the person requesting information

Full name:	
Address:	
Contact telephone number:	
Email address:	

SECTION 2: Are you the data subject?
Please tick the appropriate box and read the instructions which follow it.

YES: ☐ I am the data subject. I enclose proof of my identity (see below).
(please go to section 4)

NO: ☐ I am acting on behalf of the data subject. I have enclosed the data subject's written authority and proof of the data subject's identity and my own identity (see below).
(please go to section 3)

To ensure we are releasing data to the right person we require you to provide us with proof of your identity and of your address. Please supply us with a photocopy or scanned image (do not send the originals) of one of both of the following:

Proof of Identity
Passport/photo driving licence/national identity card/birth certificate.

Proof of Address
Utility bill, bank statement, credit card statement (no more than 3 months old); current driving licence; current TV licence; local authority tax bill, HMRC tax document (no more than 1 year old).

If we are not satisfied you are who you claim to be, we reserve the right to refuse to grant your request.

SECTION 3
Details of the data subject (if different from section 1)

Full name:	
Address:	
Contact telephone number:	
Email address:	

SECTION 4: What information are you seeking?
Please describe the information you are seeking. Please provide any relevant details you think will help us to identify the information you require.

Please note that if the information you request reveals details directly or indirectly about another person we will have to seek the consent of that person before we can let you see that information. In certain circumstances, where disclosure would adversely affect the rights and freedoms of others, we may not be able to disclose the information to you, in which case you will be informed promptly and given full reasons for that decision.

While in most cases we will be happy to provide you with copies of the information you request, we nevertheless reserve the right, in accordance with section 8(2) of the DPA, not to provide you with copies of information requested if to do so would take "disproportionate effort", or in accordance with Article 12 of the GDPR to charge a fee or refuse the request if it is considered to be "manifestly unfounded or excessive". However, we will make every effort to provide you with a satisfactory form of access or summary of information if suitable.

SECTION 5: Information about the collection and processing of data
If you want information about any of the following, please tick the boxes:

Why we are processing your personal data ☐

To whom your personal data are disclosed ☐

The source of your personal data ☐

SECTION 6: Disclosure of CCTV images
If the information you seek is in the form of video images captured by our CCTV security cameras, would you be satisfied with viewing these images?

YES ☐ NO ☐

SECTION 7: Declaration
Please note that any attempt to mislead may result in prosecution.

I confirm that I have read and understood the terms of this subject access form and certify that the information given in this application is true. I understand that it is necessary for the school to confirm my / the data subject's identity and it may be necessary to obtain more detailed information in order to locate the correct personal data.

Signed…… **Date** ……

Documents which must accompany this application:

Evidence of your identity (see section 2)

Evidence of the data subject's identity (if different from above)

Authorisation from the data subject to act on their behalf (if applicable)

Please return the completed form to Admin at: Rochdale Islamic Academy Greenbank Rd, Rochdale OL12 0HZ

Correcting Information

If after you have received the information you have requested you believe that:

- the information is inaccurate or out of date; or
- we should no longer be holding that information; or
- we are using your information for a purpose of which you were unaware;
- we may have passed inaccurate information about you to someone else;

then you should notify our Data Protection Officer at once

Appendices 4

Data Breach Reporting Template

	Report prepared by: Date: On behalf of:	*Name* *Date* *Organisation*
1	Summary of the event and circumstances	*When, what, who, summary of incident etc.*
2	Type and amount of personal data	*Title or name of the document/s; What personal information is included – Name; Address; DoB; Bank account details; description of information about an individual (health issues; case hearing notes/decisions etc)*
3	Actions taken by recipient when they inadvertently received the information	
4	Actions taken to retrieve information and respond to the breach	*Has information been retrieved? When? Has loss been contained? e.g. all emails deleted*
5	Procedures / instructions in place to minimise risks to security of data	*(communication, secure storage, sharing and exchange)*
6	Breach of procedure/policy by staff member	*Has there been a breach of policy?* *Has appropriate management action been taken?*
7	Details of notification to affected data subject Has a complaint received from Data Subject?	*Has the data subject been notified? If not, explain why not?* *What advice given to affected data subjects?*
8	Details of Data Protection training provided:	*Include date of last training prior to the incident by the staff member breaching security*
9	Procedure changes to reduce risks of future data loss	
10	Conclusion	*Serious/minor breach, likelihood of happening again*