Rosebank School

Learning together, celebrating success

Information Rights Policy and Procedure

DATE OF THIS DOCUMENT:	**MAY 2019**
Ratified by Governors:	**05/12/2019**
Frequency of Update:	**Annually**
Due for Revision:	**May 2020**
Person Responsible:	**Carina Baylis**

1.0. Introduction

1.1. The General Data Protection Regulation (GDPR) contains a number of rights for the data subject, which allows the data subject to control the use of their personal data by data controllers (the school). The rights of the individual are a central part of data protection legislation and Rosebank School is legally bound to respond to them.

1.2. The General Data Protection Regulation expands upon the rights of the individual that exist within the Data Protection Act 1998 by introducing more rights, but also changing the fundamental timeframes and expectations that the School must meet.

2.0. The Rights

2.1. The GDPR gives individuals the following rights: -

1. The right to be informed (covered as part of the School's Privacy Notice and Transparency Guidance)
2. The right of access
3. The right to rectification
4. The right to erasure
5. The right to restrict processing
6. The right to data portability
7. The right to object
8. Rights in relation to automated decision making and profiling

2.2. All Rights under the GDPR are not absolute. For this reason, the Data Protection Officer should always be consulted for advice to ensure that the school are acting appropriately in the way they deal with any request by an individual to exercise a specific right.

3.0 The Right of Access

3.1. The right of access (also known as Subject Access Requests) gives the individual the right to ask for: -

- Confirmation that the School is processing (using) their personal data
- Access to their personal data itself as well as supporting information about who their information is shared with and what it is used for.

3.2. The right of access gives an individual the right to request their own information from the School. They are not entitled to view information about another individual unless they have obtained that individual's explicit consent, unless their right to the data outweighs the rights of the other individual.

3.3. An individual may request personal data from the School on behalf of another person, for example – a child. In these cases the requester must provide the following documentation.

- Proof of identification for both the requester and the person they are requesting the information on behalf of.
- Proof of authority to act on their behalf. This may include Power of Attorney forms, signed authority from a solicitor's office or in the case of a child, proof of parental responsibility.

3.4. All documents must be redacted to remove any personal data about third parties (other people) before release. This redaction must be dip sampled and approved by the School Data Protection Lead before release to the requester.

3.5. Parents accessing their child's personal data under the GDPR are exercising the child's right of subject access on the child's behalf.

3.6. A parent or guardian does not have an automatic right to information held about their child. The right belongs to the child and the parent(s) acts on their behalf, where they have parental responsibility for the child.

3.7. In England the age at which a child reaches sufficient maturity to exercise their own right to access their information is normally 12, but this may vary amongst individuals. Once a child reaches sufficient maturity, the parent may only act with their child's consent.

3.8. Where a child is over 12 and a request is made on their behalf, the school may contact them separately to seek their signed consent for someone to access their records on their behalf. When deciding whether information about a child can be released, consideration will be given to the best interests of the child.

3.9. The school will not service a Subject Access Request for information held on a child if the child, having been deemed capable of understanding the nature of the request and the consequences of their actions, refuses to consent to this information being disclosed.

Full details of Rosebank School's Right of Access Policy is available on the school website.

4.0 The Right of Rectification

4.1. The right of rectification gives the data subject the right to request that inaccurate data held by the School is rectified or deleted.

4.2. Where the School receives a request to rectify inaccurate data, it is best practice that the personal data is restricted from use whilst an assessment of its accuracy is carried out.

4.3. All requests for Rectification of data will be referred to the Data Protection Officer at the same time they are referred to the relevant service. The DPO must approve the School's action before it is conducted.

4.4. Where the requester can manifestly prove that data is inaccurate (e.g. an address inaccurately entered) the School may ask for proof of the correct address in order to appropriately correct the mistake.

4.5. Where the requester queries whether an opinion recorded about them has any merit, the School may take the action to clearly mark the data as an opinion rather than fact. This may also mean that the School does not rectify or delete this data.

5.0 The Right to Erasure (Right to be Forgotten)

5.1. The right to be forgotten is not absolute and only applies in certain circumstances. They are: -

- The personal data is no longer necessary for the purpose which the School originally collected or used it for;
- The School are relying on consent as the lawful basis for holding the data, and the individual withdraws their consent;
- The School are relying on legitimate interests as the basis for using the personal data. The individual objects to the processing of their data, and there is no overriding legitimate interest to continue this processing;
- The School are using the personal data for direct marketing purposes and the individual objects to that processing;
- The School have processed the personal data in breach of the General Data Protection Regulation
- The law states that the personal data has to be deleted
- The School has collected the personal data through offering online services to a child.

5.2. The right to be forgotten does not apply in numerous situations, including: -

- Where the School has a statutory duty to keep the information
- Where there is a high public interest in the School keeping the information and it is used for a public function (e.g. safeguarding)
- Where the information is necessary for a legal claim

5.3. Where a right to be forgotten request is received, the Data Protection Officer must be consulted at the earliest opportunity in order to advise regarding the deletion of the personal data in question.

5.4. Some School systems will not facilitate the erasure of personal data. Where this is the case, the data must be flagged on the system as being “not to be used” and must not be included in any reports or documents produced from that system.

5.5. Where an applicant successfully applies their right to be forgotten and the School has previously shared the deleted information with another agency, the School must immediately contact the recipient agency and ask them to remove the data from their systems.

6.0. The Right of Restriction

6.1. The right of restriction gives an individual the right to ask the School to temporarily stop using their information in the following circumstances: -

- The individual disputes the accuracy of their personal data and the School are verifying the accuracy of the data.
- The data has been unlawfully used or shared and the individual chooses for the School to restrict access to the data, rather than delete it.
- The School no longer need the personal data but the individual needs the School to keep it in order to establish, exercise or defend a legal claim
- The individual has objected to the School using their data (see right to objection below) and you are considering whether your legitimate grounds override those of the individual.

6.2. Where a right to restriction (or rectification/objection) request is received, the Data Protection Officer must be consulted at the earliest opportunity in order to advise regarding the restriction of the personal data in question.

6.3. Some School systems will not facilitate the restriction of personal data. Where this is the case, the data must be flagged on the system as being “not to be used” and must not be included in any reports or documents produced from that system.

6.4. Where an applicant successfully applies their right to restriction and the School has previously shared the deleted information with another agency, the service must immediately contact the recipient agency and ask them to restrict the data on their systems.

7.0 The Right of Data Portability

7.1 The right of data portability gives the individual the right to receive any information that they have previously supplied to the School back, in a commonly used, machine readable format.

7.2. This right only applies in the following situations: -

- Where the School is using personal data with the consent of the individual involved
- Where the School is using personal data as part of a contract with the individual
- Where the use of personal data is done in automated (computerised) way

7.3. The right only applies to personal data that the individual has directly provided to the School. The School is not obliged to provide information that it has generated about the individual, only the information they initially provided to us. If the requester requires information wider than what they have provided to the School, they must make a Subject Access Request.

7.4. The requester has the right to receive their information directly, or ask the School to provide to another organisation. The requester must make their wishes clear in this regard.

7.5. Where a right to data portability request is received, the Data Protection Officer must be consulted at the earliest opportunity in order to advise regarding the restriction of the personal data in question.

7.6. The personal data requested must be provided in a commonly used, machine readable format. It may be appropriate to ask the requester for their preferred method and file format in which to receive their disclosure.

7.7. Where the personal data requested is not accessible to be removed in a portable manner, the Data Protection Officer must be informed immediately so that appropriate communication can take place with the requester and a compromise reached about the format of the disclosure.

8.0. The Right to Object

8.1. The right to object gives individuals the right to request that the School stops processing their personal data in certain circumstances.

8.2. The right to object applies in the following situations: -

- Where the School is using the individual's personal data in line with their public tasks and functions (Article 6(e) of the GDPR) or in the School's legitimate interests (Article 6(f)).
- Where the School is using the personal data for direct marketing or profiling purposes.
- Where the School is using the personal data for scientific/historical research or statistical purposes

8.3. The right to object is not absolute with regards to personal data processing by the School for its functions. In order to refuse a right to object, the School must demonstrate compelling and legitimate grounds for keeping the information. This may include grounds of public interest, safeguarding purposes or crime prevention.

8.4. If the School requires the personal data for the defending a legal claim then the requester cannot use their right to object.

8.5. Where the requester would like to object to direct marketing from the School, this request must be honoured immediately. There are no exemptions to this right. The School must remove the requester's data from all mailing lists and ensure that they receive no further marketing communications from that point.

8.6. Where a right to object request is received, the Data Protection Officer must be consulted at the earliest opportunity in order to advise regarding the application of this right.

9.0. The Right to Prevent Automated Decision Making (including Profiling)

9.1. The GDPR gives the individuals the right to object to any automated decisions being made about them that would have a significant effect. It also gives the individual the right to prevent automated profiling of them.

9.2. Automated decision making is a decision that is made about an individual without any human involvement. An example of this is a credit check before buying a product on higher purchase.

9.2. Profiling is specifically mentioned in the GDPR as automated profiling that is used to evaluate a person's behaviour to analyse or predict their actions or needs. The text specifically mentions employment, economic situation, health, personal preferences, interests, reliability, behaviour and movements (location).

9.3. The use of information must result in a decision being taken about the individual in question. If no decision is taken, the individual cannot prevent the processing using this right, they must exercise their right to object.

9.4. The School may only carry out this type of processing in the following circumstances: -

- The decision is necessary for entering into a contract with the individual(s) involved
- Authorised by law (e.g. for preventing crime or fraud)
- The individual has given their explicit consent.

9.5. If the decision making is to include sensitive (special category) personal data, then the School must have: -

- A substantial public interest in the decision being taken
- The individual's explicit consent

9.6. This use of personal data cannot be undertaken without completing a Data Protection Impact Assessment.

9.7. Where a right to preventing automated processing request is received, the Data Protection Officer must be consulted at the earliest opportunity in order to advise regarding the application of this right.

10.0 Expectations and Basic Principles

10.1 Procedure for GDPR subject rights requests

10.1.1 GDPR gives individuals a set of rights over their data:

- Access to their data
- Rectification
- Erasure
- Restriction in certain circumstances
- Portability
- Objection over the use of certain legal bases
- Rights over automated decisions

10.1.2 These rights are not absolute and are dependent on the legal basis applied for the collection or use of personal data. As a result, all requests must be assessed individually.

10.1.13 As requests need not be made to one point of contact, it is the responsibility of all staff to understand and be able to identify a Rights Request, as well as the process for escalating such requests.

10.1.4 Requests made for access to personal data must be immediately referred to the School's Data Protection Lead. All other requests should be referred to the School's DPO.

10.1.5 All requests, must follow the same basic principles in that:

- Correspondence for each request must be kept together
- Every request will be allocated a reference number
- Every request will be logged so that compliance with the timescales can be monitored
- Anyone making a request verbally or via social media will be asked to put their request in writing
- Any applicant who does not include proof of ID with their request, or where identification is not already known or readily identifies, should be asked to provide it
- Applicants will be made aware of the School's online form – and while they cannot be compelled to complete this form - it is an opportunity to explain how the rights work and to give the applicants advice.

10.2 Proof of identity

If there is any doubt about the identity of the subject (and to meet the requirement to protecting the confidentiality of data under the sixth GDPR principle), the School should request sufficient proof to establish the identity of the data subject but not an excessive level of proof. For example, sending information to an email address that you regularly use to communicate with the person may negate the need for an identity check where the data is not sensitive. Do not ask for original copies of ID.

10.3 Verbal requests

The GDPR does not specify that requests have to be made in writing – logically, this means that a request can be made verbally. A legitimate request for proof of ID will facilitate a written request in many cases.

10.4 Timescales

Once the proof of ID and proof of consent (where required and requested) have been provided, the we have one month to comply with the request. Note that this is the maximum allowable, it is not a target. If we can service the request within 1 month then we should.

10.5 Timescale Summary

- **Request from the individual** - The same date in the next month following receipt of proof of ID and (where requested) clarity over what they are asking for.
- **Request from solicitors or others representing the subject** - The same date in the next month following receipt of consent & entitlement and (where requested) clarity over what they are asking for.
- **Requests from family for records of deceased -** GDPR does not apply to these requests) - As soon as is reasonable after receipt of proof of status (e.g. executor or closest surviving relative)

10.6 Extending Timescales

The timescale can be extended by up to two months if the request is complex, or if there are multiple requests from the same person. The reasons for extending the deadline should be clearly set out in the reply. The complexity must be caused by the request itself, rather than problems with the organisation's internal records management and systems. The applicant must be informed of any delay before the end of the first month and told when their request will be answered.

Any decision to extend timescales must be referred to the School's DPO to assess.

10.7 Fees

The default is that no fee can be charged for dealing with a request – this includes time taken to locate information, take any requested action, redact irrelevant data or references to other individuals where necessary, scanning, printing and postage where relevant.

There are only two situations where a charge can be made

- If the request is manifestly unfounded

- If the request is manifestly excessive

In both cases, the decision to charge a fee should usually be based on the nature of the request – any decision to look at correspondence or activities outside the request itself should be clearly documented.

Any decision to charge a fee should be referred to the DPO who will assess under what category a fee may be charged:

10.8 Manifestly unfounded

- The applicant has asked for the same thing before and received it or a legitimate refusal
- The request involves a complex, detailed search and there is no evidence that they have a relationship with the organisation
- There is evidence that the applicant has made the request to waste time or distract the resources of the organisation from another matter

10.9 Manifestly excessive

- The request explicitly includes backups or other data sources that are not live
- The request covers a large amount of data and the applicant refuses to limit the scope

10.10 General Procedure

Depending on the request, either the DPL will co-ordinate the response to the individual, however, this will necessitate individuals identifying where information may be held and how and why it is used.

• If information is held (or likely to be held) in more than one area, we may consider asking applicant for further information, such as:

- who have they have dealt with
- what information do they want?
- do they have any identifiers or reference numbers which may assist in the search?

• If not already been provided, we will ask applicant for proof of their identity –

- a copy of driving licence OR
- current passport OR
- current utility bill (not a mobile phone or store card)
- if the applicant cannot provide any of these, ask what other proofs of ID they can provide

• If the data is about a child, we will ask for:

- copy of child's birth certificate OR
- current child's passport

AND

- proof of parent's identity

- if there is any doubt about whether the parent is entitled to information, we may request a copy of child benefit letter or payments to establish that the child is living with the parents
- If the data is about the child who does not live with the applicant parent, we may contact any professionals involved with the child with whom we have contact (e.g. health, social care) to consider whether there is any court order or other reason why supplying information is not in the child's interests. If no professional can be contacted, we may contact the parent with whom the child lives. The other parent does not have a veto, but the interests of the child are paramount.

• If the applicant is a solicitor, proofs of identity can be requested, but signed consent from the subject for the solicitor to make the request on their behalf must be provided.

• Once the above has been received, the request is valid, and the statutory timescales for compliance begin. The request will be logged and an acknowledgement sent.

• When information is requested from services, they will be given a maximum of 15 days to provide the information, before the request is escalated to the senior manager.

• A nominated member of the team will chase the request after 20 days to ensure that the data is supplied with enough time to consider the issues.

• Unedited copies of relevant documents should be provided to the Disclosures Team from teams that hold the data – originals will be accepted only in exceptional circumstances. The transfer of original copies of data is an unnecessary security risk that should generally be avoided.

• If a child is likely to have capacity to make decisions, consideration will be given to whether the child may have rights to the information. A child who has capacity to understand the implications of their data may be entitled to have access to it – decisions should always be taken in the child's interests. If an adult does not have capacity, the decision should be referred to an appropriate professional, or a person who has power of attorney for the subject.

10.11 Exemptions

The DPO should be consulted on whether an exemption applies, and whether it is necessary to remove data to protect some other interest or refuse a request.

11.0 Individual Rights

11.1 Subject access issues

The applicant is entitled to receive:

• the data itself

• the purposes of the processing;

• the categories of personal data being processed;

• the recipients of data

• retention period of the data

• information about the subject's rights to request rectification, restriction or objection

• the right to lodge a complaint with a supervisory authority;

• any available information about the source of the personal data

• information about significant instances of automated decision-making, including profiling

11.2 Withholding information about third parties

Information about third parties – family members, friends or others - should be disclosed where it is fair and reasonable in all the circumstances to do so. For example, where the data would clearly be known to the subject, or is already be in the public domain, there is no need to edit the information out. Care should be taken to ensure that data is not private, and that disclosure will not put the third party at any risk. The names of professionals involved in the care of or decisions about the individual should not normally be removed.

11.3 Confidential information

If information about the person was provided in confidence (e.g. a complaint or as part of an investigation conducted in confidence), information can be withheld. The DPO should decide whether the duty of confidence outweighs the person's subject access rights. They will consider whether to ask the third party's permission to disclose. Withheld information should be retained to make sure that it is possible to justify any refusal should there be any complaints.

11.4 Sending out information

• Information should be sent out by recorded delivery, and the envelope properly sealed.

• Copies of disclosed records, as well as any information withheld, should be retained with all correspondence relevant to the request.

The DPO will record the reasons for any use of exemptions. The applicant does not need to be informed that exemptions have been used.

Teams will be advised that concerns about the harm caused by disclosure must be raised by an appropriate professional before supplying copies of the records.

Unless concerns are raised, the DPO will assume that disclosure should go ahead.

11.5 Restriction issues

If the restriction request is valid, a marker must be added to the relevant records stating that the information should not be accessed. The DPO should determine whether it is necessary to limit access to the personal data rather than simply add a marker

If request is to be refused, the DPO must document which exemption applies.

- Important public interest
- Need to protect the rights of another person
- The establishment exercise or defence of legal claims
- DP Act 2018 Exemption

11.6 Right to be forgotten issues

A person has a right to request that data is erased.

The DPO is responsible for ensuring that data is erased, and evidence for the erasure must be retained. Evidence of erasure must be made available to the Data Protection Officer / DP Lead on request.

If request is to be refused, the DPO must document which exemption applies and retain evidence of the decision.

- Freedom of expression
- Legal obligation, public interest task, official authority
- Public health / public interest
- Archiving, scientific or historical research purposes or statistical purposes
- Establishment, exercise or defence of legal claims
- DP Act 2018 Exemption

11.7 Portability issues

The DPD is responsible for identifying the extracting of portable data.

It will be disclosed to the applicant using secure email or other secure file transfer methods.

The data subject has the right to request that the portable personal data is transmitted directly from one controller to another, where this is technically feasible. A refusal to transfer the data should be documented by the DPO.

11.8 Objection issues

A person has a right to object to processing where the legal basis is public interest task or official authority, or legitimate interests.

The DPO should consider such objections, taking into account the original basis for the decision (including the balancing exercise carried out for legitimate interests). They should consider any particular issued raised by the applicant about why the processing should cease. If refusing the request, the DPO should be able to demonstrate why the processing is necessary despite the objection in relation to the person concerned.

The DPO must document any decision to override the objection of the individual, including the reasons why the importance / significance of the processing is deemed to override the objection request.

11.9 Automated issues

A person should not be subject to a wholly automated decision except in certain limited circumstances – where the decision is necessary for a contract, where it is authorised by law, or where explicit consent has been obtained.

Where a person objects to a wholly automated decision, the DPO must ensure that that the decision is made by an officer and the individual is allowed to make representations and have access to information about how the decision is made.

Where this will not be provided, the reasons should be documented by the DPO.

11.10 Transfer Issues

Where a person successfully requests rectification, restriction or erasure, and their request should be transferred to any other data controller to which the data in question has been disclosed. The reasons for any refusal to do so (impossible or disproportionate effort) should be clearly documented.

11.11 Complaints and challenges

• If the applicant has legitimate cause to complain that information is missing from the response, or is held and should have been included, this should be provided as soon as possible, unless an exemption has been used.

• Any inaccuracy that the individual identifies in the information that has been supplied should be corrected or amended as soon as possible. Original records should not be altered to obscure the original information

• Applicants should be advised to use the School's complaints procedure if they are not satisfied.