GDPR Individual Rights and Complaints Policy

Developed from Oldham Council Policy – January 2019
Reviewed Sept 2020

1. Objectives

1.1. We recognise the need for legal compliance and accountability and endorse the importance of the rights of data subjects and the requirement to provide a complaints mechanism.

1.2. This policy sets out the key requirements in relation to the exercise of individual rights and complaints to which we are fully committed

2. Scope

2.1. In order to fulfil its statutory and operational obligations we have to collect, use, receive and share personal, special personal and crime personal data about living people, e.g.

- Pupils and their families
- current, past, prospective employees
- clients and customers
- contractors and suppliers
- Governors members of the public (adults & children)

2.2. This policy covers the obligations to respond to individual rights and complaints in relation to personal data, regardless of data age, format, systems and processes purchased, developed and managed by/or on behalf of us and any person directly employed or otherwise by us.

2.3. This policy reflects the commitment to data protection compliance to both UK and EU legislation, in particular the Data Protection Act 2018, the EU General Data Protection Regulation 2016 (GDPR) and the EU Law Enforcement Directive 2016 (LED).

3. Policy

3.1. Data Protection Officer (DPO): We will appoint a data protection officer who will be the key contact for the provision of independent advice on all things data protection. The DPO will provide advice and support when dealing data subject enquiries and communications with the Information Commissioners Office.

Data Protection Officer

Barbara Mulvihill

LA Data Protection Officer on behalf of Burnley Brow Community School:

West Street

Oldham OL1 1UT

Email: DPO@oldham.gov.uk

Tel: 0161 770 1311

3.2. Individual Rights: Data subjects have the following rights: (see Appendix 1 for more information and the guide to individual rights)

- The right to be informed
- The right of access
- The right to rectification
- The right to erasure
- The right to restrict processing
- The right to data portability
- The right to object
- Rights in relation to automated decision making and profiling
- The right to be informed in the event of a data security incident that poses a high risk

Plus data subjects are also able to:

- seek a review/complain to the DPO
- complain to the Information Commissioners Office (ICO)
- seek judicial remedy, including compensation through the courts

These requests may be made verbally or in writing.

If a request is made verbally and the applicant refuses or is unable to put it in writing, it would be good practice provide the applicant with a written summary of your understanding of the request and ask them to confirm the summary is correct.

In all cases where there is any doubt as to the requestor's identity two proofs of identification will be necessary to confirm the requestor is who they say they are.

Where a request is 'manifestly unfounded, excessive or repetitious' the law says we can either:

- Charge a fee to respond or

- Refuse the request on one or more of these grounds

As a matter of policy, where we determine a request is manifestly unfounded, excessive of repetitious we intend to refuse the request. Where we refuse a request the onus rests on us to demonstrate that the request falls within the threshold for relying on one or more of these grounds.

3.3. Timescales for Response to individual rights requests and complaints: We will provide a written response within one calendar month* that explains the outcome of our decision with regards to an individual query/request and/or complaint.

The time starts the first day after receipt of the enquiry where we are satisfied with verification of the data subject's identity**.
This time can be extended to 2 calendar months where the case is complex or voluminous and the data subject has been informed of this within one calendar month of the original enquiry. In the event of a serious data breach, we have an obligation to inform the data subject without undue delay if this poses a high risk for their privacy risks. This could mean that is some cases, the data subject is entitled to know before the 72 hour deadline for notifying the ICO.

*Note: the response needs to be within 21 days where the request is in relation to objection to processing, and in the event of a serious data breach, as soon as possible
**Note: and information to locate the personal data where the request is in relation to data subject access or objection to processing.

3.4. Reasons for lapsing requests: If ID and necessary information to locate requested information or to clarify what the requestor is asking, is not received then it may be necessary to 'lapse' the request if this is not received after 3 months.

3.5. Reasons for refusing requests: In addition to requests which may be considered manifestly unfounded and excessive requests etc. as outlined in 3.2, there are other likely exemptions that allow us to partially or wholly comply with individual rights. These are:

- Rights of other individuals
- Crime and taxation
- Immigration
- Determined by law, and legal proceedings
- Public protection and regulatory functions
- Parliamentary privilege
- Judicial appointments/proceedings
- Other people's data unless consent, or reasonable without consent
- Self-incrimination

- Corporate finance
- Management forecasts
- Negotiations
- Confidential references
- Exams
- Special purposes e.g. artistic, literary, journalistic
- Research and statistics
- Archiving in the public interest

If the personal data is in relation to law enforcement, the exemptions include:

- Prejudice/obstruction to prevention, detection, investigation, prosecution of crime
- In the interests of public and national security and rights and freedoms of individuals, e.g. privacy

3.6. The response to the data subject: The response to the data subject needs to contain the following:

- Acknowledgement of the request/enquiry made
- Whether or not we are able to comply with what the requestor is seeking, and an explanation of the reasons why not.
- If we are unable to comply with what the request is seeking, and an explanation of the reasons why.
- The right to complain to the ICO

3.7. Complaints: Details of the complaints process can be found on the school website.

4. Assessment and Monitoring

4.1. An assessment of compliance with requirements will be undertaken in order to provide:

- Assurance
- Gap analysis of policy and practice
- Examples of best practice
- Improvement and training plans

Commented [BM1]: This would be good practice and help you demonstrate that you comply with the legislation and in particular the accountability principle, ie, where the onus is on the data controller to actively evidence compliance. Feel free to amend this section as suits your environment

Commented [h2R1]:

4.2. Reports will be submitted to the Senior Management Team and Audit Committee.

5. Responsibilities and Approvals

5.1. **Governing Body**:

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

5.2. **Headteacher**:

The Headteacher acts as the representative of the data controller on a day-to-day basis and is responsible for the approval of this policy.

5.3. Data Protection Officer:

The data protection officer will be the key contact for the provision of independent advice on all things data protection. The DPO will provide advice and support when dealing data subject enquiries and communications with the Information Commissioners Office

5.4. Governors/Employees:

All Governors and staff, whether permanent, temporary or contracted, including students, contractors and volunteers are responsible for ensuring they are aware of the data protection legislation requirements and for ensuring they comply with these on a day to day basis. Where necessary advice, assistance and training should be sought. Any breach of this policy could result in disciplinary action or could constitute a criminal offence

Appendix 1 – Rights of Individuals

The right to be informed

Data subjects have the right to be informed about the collection and use of their personal data, this will primarily be via a privacy notice

The right of access

Data subjects have the right to request access to their own personal data and be provided with an intelligible permanent copy this is within 1 calendar month of receipt of appropriate ID and any required supporting information. This applies to any personal data held that is not covered by the Pupil Information Regulations which allow those with parental responsibility to access their child's pupil record.

The right to rectification

Data subjects have the right to request the rectification of inaccurate or incomplete personal data. This request could be fulfilled by the provision of a supplementary statement. Where the personal data needs to be retained as part of the record, for evidence purposes, instead of rectifying it, its use could be restricted.

If you have shared/disclosed this personal data with another body, you must notify those recipients of the rectification/restriction of the information.

The right to erasure

Data Subjects have the right to be 'forgotten' but this does not apply in all circumstances.

It does apply where:

- the personal data is no longer necessary for the purpose which you originally collected or processed it for
- you are relying on consent as your lawful basis for holding the data, and the individual withdraws their consent
- you are relying on legitimate interests as your basis for processing, the individual objects to the processing of their data, and there is no overriding legitimate interest to continue this processing
- you are processing the personal data for direct marketing purposes and the individual objects to that processing
- you have processed the personal data unlawfully
- you have to do it to comply with a legal obligation
- you have processed the personal data to offer information society services to a child.

If you process data collected from children you should give particular weight to any request for erasure if the processing of the data is based upon consent given by a child – especially any processing of their personal data on the internet. This is still the case when the data subject is no

longer a child, because a child may not have been fully aware of the risks involved in the processing at the time of consent.

If you erase the personal data requested you need to notify any recipients you have shared/disclosed this information with, and if you have made the information public, then endeavour to remove it from the public domain/internet.

It does **not** apply in the following circumstances:

- to exercise the right of freedom of expression and information
- to comply with a legal obligation
- for the performance of a task carried out in the public interest or in the exercise of official authority
- for archiving purposes in the public interest, scientific research historical research or statistical purposes where erasure is likely to render impossible or seriously impair the achievement of that processing; or
- for the establishment, exercise or defence of legal claims.

In addition, the right does not apply to special personal data where:

- it is necessary for public health purposes in the public interest (e.g. protecting against serious cross-border threats to health, or ensuring high standards of quality and safety of health care and of medicinal products or medical devices); or

- it is necessary for the purposes of preventative or occupational medicine (e.g. where the processing is necessary for the working capacity of an employee; for medical diagnosis; for the provision of health or social care; or for the management of health or social care systems or services). This only applies where the data is being processed by or under the responsibility of a professional subject to a legal obligation of professional secrecy (e.g. a health professional).

The right to restrict processing

Data Subjects have the right to request restriction/suppression of processing, but this does not apply in all circumstances. When processing is restricted, you are permitted to store the personal data, but not use it. This may be an alternative to erasure or rectification and it is unlikely that a restriction would be in place indefinitely, but could be temporary whilst issues with the personal data are resolved. If you decide to remove the restriction you must tell the data subject **before** you continue to process the data**.**

The rights applies where

- the data subject contests the accuracy of their personal data and you are verifying the accuracy of the data
- the data has been unlawfully processed and the data subject opposes erasure and requests restriction instead
- you no longer need the personal data but the data subject needs you to keep it in order to establish, exercise or defend a legal claim

- the data subject has objected to you processing their data on grounds that you are relying on legitimate interests as your basis for processing, and you have no overriding legitimate interest to continue this processing or are processing it for profiling purposes.

Although this is distinct from the right to rectification and the right to object, there are close links between those rights and it would be good practice to automatically restrict processing whilst considering its accuracy and legitimate grounds of processing.

Ways of restricting processing may include, but are not limited to:

- temporarily moving the data to another processing system;
- making the data unavailable to users; or
- temporarily removing published data from a website.

The data should not be erased or changed whilst restricted and no further processing should take place during this time except to store it, unless:

- you have the individual's consent;
- it is for the establishment, exercise or defence of legal claims;
- it is for the protection of the rights of another person (natural or legal); or
- it is for reasons of important public interest.

If you restrict the processing of personal data you need to notify any recipients you have shared/disclosed this information to.

The right to data portability

Data Subjects have the right to request for data portability, which allows data subjects to obtain and reuse their personal data for their own purposes across different services. This involves moving, copying, and/or transferring personal data easily across IT environments safely and securely

The right to data portability only applies:

- to personal data a data subject has provided to us;
- where the processing is based on the individual's consent or for the performance of a contract; and
- when processing is carried out by automated means.

You must provide the data subject with their own personal data in a commonly machine readable form, e.g., csv files. If the data subject requests it, and it is technically feasible, you need to transmit this data to another organisation. If the personal data concerns more than one individual, you must consider whether providing the information would prejudice the rights of any other individual e.g. privacy, data protection, confidentiality etc.

The right to object

Data subjects have the right to object to:

- Processing based on legitimate interests or the performance of a task in the public interest/exercise of official authority (including profiling);

  You must stop processing the personal data unless:

  - you can demonstrate compelling legitimate grounds for the processing, which override the interests, rights and freedoms of the individual; or
  - the processing is for the establishment, exercise or defence of legal claims

- Direct marketing (including profiling);

  You must stop processing personal data for direct marketing purposes as soon as you receive an objection. There are no exemptions or grounds to refuse.

- Processing for purposes of scientific/historical research and statistics.

  If you are conducting research where the processing of personal data is necessary for the performance of a public interest task, you are not required to comply with an objection to the processing.

Rights in relation to automated decision making and profiling

Data Subjects have the following rights where we make automated decisions about them or make decisions about them via profiling.

Automated decisions means – making a decision solely by automated means without any human involvement

Profiling means - automated processing of personal data to evaluate certain things about an individual

This type of processing can only be carried out for decision making that is:

- necessary for the entry into or performance of a contract; or
- required by law; or
- based on explicit consent

The data subject should be informed as part of their privacy notice that this is taking place and the logic to the decision making process. They should also be advised how to request human intervention in the decision making process.

The right to be informed in the event of a data security incident which poses a high risk

Data subjects have the right to be informed if there is a serious data breach in relation to their personal data