



Individual Rights & Complaints Policy

Document Control Information	
Document Title	Individual Rights and Complaints Policy
Organisation / Site	New Bridge Multi Academy Trust
Review Period :	Every 2 years
Document Owner and Reviewer:	Director Operations
Approval Committee	Trustees

Revision and Approval History					
Author	Summary of changes	Issue	Date Applicable From	Approved by	Date of Next Review
R Righini	Policy re new GDPR rules	1	31/05/2018	Trustees	31/08/2020
R Righini	Changes to clarify day 1 of timeline	2	31/05/2019	Trustees	31/08/2021
R Righini	Review – no changes	3	30/04/2021	Trustees	30/04/2023
R Righini	Review – minimal changes to reflect EU exit.	4	01/12/2022	Trustees	01/12/2024

Equality Impact	
Statement	<p>We welcome feedback on this document and the way it operates. We are interested to know of any possible or actual adverse impact that may affect any groups in respect of any of the equalities act 2010 protected characteristics.</p> <p>The person responsible for equality impact assessment for this document is the Director of Equality and Diversity.</p>
Screening	<p>This document has been screened by the Equality Team and the impact has been assessed as:</p> <p> <input type="checkbox"/> Not applicable <input type="checkbox"/> Low <input type="checkbox"/> Medium <input type="checkbox"/> High </p>

Equality Impact Assessment Form

To be completed by document author / lead person

Title of document		Individual Rights and Complaints Policy			
Organisation / Site	New Bridge Multi Academy Trust	Person completing form	Rita Righini	Date	01/12/2022
Does the process affect one group less or more favourably than another on the basis of:					Yes / No
Age refers to a person belonging to a particular age					No
Disability A person has a disability if s/he has a physical or mental impairment which has a substantial and long-term adverse effect on that person's ability to carry out normal day-to-day activities.					No
Gender reassignment The process of transitioning from one gender to another.					No
Marriage and civil partnership Marriage and civil partnership means someone who is legally married or in a civil partnership. Marriage can either be between a man and a woman, or between partners of the same sex. Civil partnership is between partners of the same sex.					No
Pregnancy and maternity Pregnancy is the condition of being pregnant or expecting a baby. Maternity refers to the period after the birth, and is linked to maternity leave in the employment context. In the non-work context, protection against maternity discrimination is for 26 weeks after giving birth, and this includes treating a woman unfavourably because she is breastfeeding					No
Race Race can mean your colour, or your nationality (including your citizenship). It can also mean your ethnic or national origins, which may not be the same as your current nationality. For example, you may have Chinese national origins and be living in Britain with a British passport. Race also covers ethnic and racial groups. This means a group of people who all share the same protected characteristic of ethnicity or race.					No
Religion and belief Religion has the meaning usually given to it but belief includes religious and philosophical beliefs including lack of belief (e.g. Atheism). Generally, a belief should affect your life choices or the way you live for it to be included in the definition.					No
Sex A man or a woman.					No
Sexual orientation Whether a person's sexual attraction is towards their own sex, the opposite sex or to both sexes.					No
If you have identified potential discrimination, please explain how the exception is valid, legal and/or justified? enter					

To be completed by EIA Lead

If potential discrimination has been identified, are the exceptions valid, legal and/or justified?		N/A
Does this policy / service / procedure need adjusting to remove any disadvantage identified or to better promote equality?		No
Impact Assessment Result (See tool below)	Low impact	
Date assessed.	01/12/2022	
High Impact The policy or process has a major impact on equality	Medium Impact The policy or process has an impact on equality	Low Impact The policy or process might have an impact on equality
There is significant potential for, or evidence of adverse impact. The policy has consequences for or affects significant numbers of people	There is some evidence to suggest potential for, or evidence of adverse impact. The policy has consequences for or affects some people	There is little evidence to suggest that the policy could result in adverse impact The policy has consequences for or affects few people

1. Purpose

- 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 of Policy

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

3. Reason for Review

- 3.1. This policy was reviewed as a result of EU exit..

4. Aim(s)

- 4.1. 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.
- 4.2. This policy reflects the commitment to data protection compliance, in particular the Data Protection Act 2018, the UK General Data Protection Regulation 2016 (UKGDPR).

5. Policy

- 5.1. 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 with data subject enquiries and communications with the Information Commissioner's Office.

Data Protection Officer on behalf of New Bridge Multi Academy Trust:
Justin Hardy
West Street
Oldham
OL1 1UT

Email: DPO@oldham.gov.uk

Requests can also initially be made to the data control lead for the trust, currently Rita Righini who may refer the request to appropriate colleagues or the DPO for advice and guidance.

- 5.2. **Individual Rights:** Data subjects have the following rights: (see Appendix 1 for more information and the guide to individual rights)
 - 5.2.1. The right to be informed
 - 5.2.2. The right of access
 - 5.2.3. The right to rectification
 - 5.2.4. The right to erasure
 - 5.2.5. The right to restrict processing
 - 5.2.6. The right to data portability

- 5.2.7. The right to object
- 5.2.8. Rights in relation to automated decision making and profilin
- 5.2.9. 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:

- 5.2.10. seek a review/complain to the DPO
- 5.2.11. complain to the Information Commissioner's Office (ICO)
- 5.2.12. seek judicial remedy, including compensation through the courts
- 5.2.13. These requests may be made verbally or in writing.
- 5.2.14. 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.
- 5.2.15. 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.
- 5.2.16. Where a request is 'manifestly unfounded, excessive or repetitious' the law says we can either:
 - 5.2.16.1. Charge a fee to respond or
 - 5.2.16.2. Refuse the request on one or more of these grounds
- 5.2.17. 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.

5.3. Timescales for Response to individual rights requests and complaints:

- 5.3.1. 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
- 5.3.2. the time starts the day of receipt of the enquiry where we are satisfied with verification of the data subject's identity*.
- 5.3.3. 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.
- 5.3.4. 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 in some cases, the data subject is entitled to know before the 72 hour deadline for notifying the ICO
- 5.3.5. *Note: and information to locate the personal data where the request is in relation to data subject access or objection to processing.

- 5.4. 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.
- 5.5. 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:
- 5.5.1. Rights of other individuals
 - 5.5.2. Crime and taxation
 - 5.5.3. Immigration
 - 5.5.4. Determined by law, and legal proceedings
 - 5.5.5. Public protection and regulatory functions
 - 5.5.6. Parliamentary privilege
 - 5.5.7. Judicial appointments/proceedings
 - 5.5.8. Other people's data unless consent, or reasonable without consent
 - 5.5.9. Self incrimination
 - 5.5.10. Corporate finance
 - 5.5.11. Management forecasts
 - 5.5.12. Negotiations
 - 5.5.13. Confidential references
 - 5.5.14. Exams
 - 5.5.15. Special purposes eg, artistic, literary, journalistic
 - 5.5.16. Research and statistics
 - 5.5.17. Archiving in the public interest
- 5.5.18. If the personal data is in relation to law enforcement, the exemptions include:
- 5.5.18.1. Prejudice/obstruction to prevention, detection, investigation, prosecution of crime
 - 5.5.18.2. In the interests of public and national security and rights and freedoms of individuals, eg, privacy
- 5.6. The response to the data subject: The response to the data subject needs to contain the following:
- 5.6.1. Acknowledgement of the request/enquiry made
 - 5.6.2. Whether or not we are able to comply with what the requestor is seeking, and an explanation of the reasons why not.
 - 5.6.3. If we are unable to comply with what the request is seeking, and an explanation of the reasons why.
 - 5.6.4. The right to complain to the ICO
- 5.7. Complaints: please see our complaints policy

6. Sources and references

- 6.1. Data Protection Act

7. Other useful documents

- 7.1. Subject Access Request Policy
- 7.2. Freedom of Information Policy
- 7.3. Privacy Notice Policy
- 7.4. Equality Policy
- 7.5. Publication Scheme
- 7.6. Complaints Policy
- 7.7. Data sharing policy

8. Monitoring

- 8.1. This policy will be monitored through the MAT's accountability framework.
- 8.2. An assessment of compliance with requirements will be undertaken in order to provide:
 - 8.2.1. Assurance
 - 8.2.2. Gap analysis of policy and practice
 - 8.2.3. Examples of best practice
 - 8.2.4. Improvement and training plans

Reports will be submitted to the Governing Body / Trust Board

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 (eg 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 (eg 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 (eg 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, eg, 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 eg, 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