



Special Personal Data – Additional Data Protection Policy

Document Control Information					
Document Title		Special Personal Data – Additional Data Protection 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	New policy	1	10 th June 2015	Trustees	10/06/2017
R Righini	Policy review no changes	2	31 st August 2017	Trustees	31.08/2019
R Righini	Policy review re new GDPR rules	3	28 th May 2018	Trustees	28/05/2020
R Righini	Doc review no changes	4	01/09/2020	n/a	31/08/2022
R Righini	Doc review minimal changes to reflect EU changes	5	01/12/2022	n/a	30/11//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		Special Personal Data – Additional Data Protection 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.	There is some evidence to suggest potential for, or evidence of adverse impact.	There is little evidence to suggest that the policy could result in adverse impact
The policy has consequences for or affects significant numbers of people	The policy has consequences for or affects some people	The policy has consequences for or affects few people



1. Purpose

- 1.1. The purpose of this policy is to set out the additional safeguards that apply to these categories of data and the controls in place to ensure that it is collected, used and shared appropriately and responsibly.
- 1.2. In order to fulfil our statutory and operational obligations, it will be necessary to collect, use, receive and share personal data that because of its sensitive nature requires careful handling and protection. We will endeavour to strike the right balance between our need as a data controller to act in the public interest while at the same time respecting the rights and freedoms of the individuals to whom the personal data relates.
- 1.3. This policy reflects the commitment to data protection compliance and the privacy elements of human rights legislation. In particular this includes:
 - 1.3.1. the UK General Data Protection Regulation 2016 (UKGDPR) as supplemented by the Data Protection Act 2018 (DPA 2018)
 - 1.3.2. the UK Human Rights Act 1998.

2. Scope of Policy

- 2.1. This policy covers all aspects of handling special category data and sensitive processing regardless of age, format, systems and processes used, developed and managed by us. This includes processing by persons directly employed by us and any other persons instructed under contract to act on our behalf.
- 2.2. Special category data means personal data revealing:
 - 2.2.1. racial or ethnic origin;
 - 2.2.2. religious or philosophical beliefs;
 - 2.2.3. political opinions or trade-union membership;
 - 2.2.4. the processing of genetic data or biometric data for the purpose of uniquely identifying a natural person;
 - 2.2.5. data concerning health
 - 2.2.6. a person's sexual life or sexual orientation
 - 2.2.7. criminal conviction or offence data

3. Aim(s)

- 3.1. We recognise the need for legal compliance and accountability and endorse the importance of the integrity, availability, confidentiality and security arrangements to safeguard personal data. We also recognise that there are times that personal data is shared with, and/or received from other organisations and that this needs to be in accordance with the law.
- 3.2. This policy sets out the key data protection obligations and accountability to which we are fully committed in relation to:
 - 3.2.1. general processing
 - 3.2.2. the processing of special categories of personal data (including criminal conviction and offence data)



within the scope of the UK General Data Protection Regulation (UKGDPR)

- 3.3. We aim for all stakeholders to have an informed knowledge of the ways in which the MAT uses and processes data. In addition, we aim for all data users to be sufficiently informed about what information can and cannot be lawfully processed and shared.

4. Policy

- 4.1. When determining Data Protection Officer (DPO): We will appoint a data protection officer who will be the key contact for the provision of independent advice for all matters relating to data protection compliance. The DPO will be responsible for ensuring that we are appropriately registered with the Information Commissioner's Office (ICO) and assist in facilitating the mandatory Record of Processing Activities (ROPA), to be made available to the ICO upon demand.

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

Email: DPO@oldham.gov.uk

- 4.2. **Data Protection Principles:** There are six data protection principles, and these provide the framework for ensuring that personal data is:

- 4.2.1. *(a) processed lawfully, fairly and in a transparent manner*

This means identifying the legal power, duty or function underpinning the reason for the processing and the appropriate data protection condition(s) relied on.

It also means that privacy notices must communicate key information, including why and what types of data are to be collected, used and shared in order to satisfy transparency requirements.

- 4.2.2. *(b) processed for an explicit and specific purpose and not processed for other incompatible purposes*

This means personal data collected for one purpose cannot be used for unrelated purposes unless the law expressly permits this. An exception applies for scientific/historical/statistical research and archiving in the public interest.

- 4.2.3. *(c) adequate, relevant and limited to what is necessary for the purpose*
This principle aims to ensure that only the minimum necessary personal data is collected and used.

- 4.2.4. *(d) accurate and, where necessary, kept up to date; ensuring that personal data that are inaccurate, are erased or rectified without delay*
This principle requires those responsible for the processing to ensure that the personal data is accurate and up to date, including notifying recipients so that any errors are corrected.

- 4.2.5. *(e) keep no longer than necessary in identifiable form*
This principle requires that personal data is not stored in identifiable form for longer than is necessary. An exception applies for



scientific/historical/statistical research and archiving in the public interest.

4.2.6. *(f) protection of the personal data using appropriate technical or organisational measures*

This principle requires those responsible, including those instructed under contract, to ensure that personal data is protected from unauthorised access and misuse and that the technical and organisational measures take account of the harm that could be caused if control of the data were to be lost or compromised.

4.3. **Accountability Obligation:** We are committed to observing and to demonstrating its compliance with all the data protection principles.

In relation to lawful processing, we will ensure that it identifies appropriate data protection conditions.

4.4. **Data Privacy Impact Assessments (DPIA):** are an important vehicle in ensuring that we integrate data protection by design and default into our technical systems and day to day business operations by embedding privacy risk considerations into new and changes to systems and business processes. These assessments must take place where there is a high risk to the privacy rights and freedoms of a data subject. Examples where these are likely to be required include but are not limited to new systems and processes, new or different uses of personal data. Where a high risk is identified the DPO must be consulted before any new or changed processing is introduced to ensure adequate risk mitigation measures are implemented. Where risks are high and not adequately mitigated a referral to the ICO must be made.

4.5. **Data Collection, Use and Disclosure:** We collect personal data directly from pupils/parents/staff/governors/trustees and others as well as receiving it from or sharing it with relevant third parties such as public sector and regulatory organisations, private and voluntary sector organisations, complainants etc.

4.6. **Commitments:** As a data controller we are committed to:

4.6.1. only handling personal data lawfully and only to the extent it is necessary to do so.

4.6.2. not unnecessarily relying on consent where an alternative legal basis is available for processing personal data. If consent is the appropriate lawful basis, we acknowledge that valid consent must be freely given, fully informed and capable of being withdrawn. Where an individual is unable due to age, capacity or other reasons to give consent directly, consent will be sought from an appropriate person eg, parent, guardian, legal representative etc.

4.6.3. only sending promotional or marketing material with consent/or existing business relationship.

4.6.4. providing data subjects with privacy notices that explain why the personal data is required and how individuals can exercise their personal data rights.



- 4.6.5. protecting personal data but in the event of a personal data security breach, resulting in a high risk to the data subject(s) undertake to notify individuals and/or the ICO as appropriate.
 - 4.6.6. assisting individuals to exercise their personal data rights, and to responding within the statutory time limits and providing a complaints process.
 - 4.6.7. ensuring personal data is subject to appropriate retention and security controls taking into account the purpose of processing, the nature of the data and the information risks.
 - 4.6.8. ensuring that when sharing and disclosing personal data this is undertaken within the parameters of the law to prevent misuse, unauthorised access to personal data. A record will be kept and where appropriate information sharing agreements (ISA) will be developed in line with the ICO Data Sharing Code of Practice. Where the sharing involves a joint controller relationship, the ISA will identify the lead controller responsible for specified processing activities and for managing individual rights. Where appropriate, DPIA's will be undertaken in advance of the sharing/disclosure.
 - 4.6.9. ensuring our Records of Processing Activities (RoPA) are maintained
 - 4.6.10. ensuring that processing of personal data within our supply chains includes the contractual clauses required by law and that processing is only undertaken in accordance with our instructions.
 - 4.6.11. not transferring personal data outside of the United Kingdom to countries not covered by the UK adequacy regulations, unless the appropriate safeguards and controls are in place. This may include ensuring a transfer impact assessment has been completed, a contract is in place including the ICO authorised contract clauses, the receiver has a certification under an approved certification scheme, and/or an international data transfer agreement is in place.
 - 4.6.12. co-operating and providing information to the ICO and other regulatory bodies in pursuance of any investigation or enforcement action.
- 4.7. **Offences:** The data protection legislation contains specific offences. It is an offence:
- 4.7.1. for a person knowingly or recklessly, without the consent of the data controller to:
 - 4.7.1.1. obtain or disclose personal data
 - 4.7.1.2. procure the disclosure of personal data to another person
 - 4.7.1.3. retain it without the consent of the original data controller
 - 4.7.1.4. offer to sell or buy the personal data obtained
 - 4.7.2. or a person knowingly or recklessly to re-identify information that is de-identified personal data without the consent of the controller, or to knowingly or recklessly handle such data.
 - 4.7.3. To alter, deface, block, erase, destroy or conceal information with the intention of preventing disclosure of all or part of the information that the



data subject making the request for access or portability would have been entitled to receive.

- 4.7.4. To require a data subject to provide or give access to information obtained via data subject access in relation to health, conviction/caution records for the purpose of recruitment, continued employment, in connection with provision of goods and service to the public. In summary, a data subject should not be obliged to make a data subject access request for this type of information as a condition/implied condition of employment or contract.
- 4.7.5. To intentionally obstruct or give false information to the ICO in the exercise of its powers under information notices and/or warrants.

5. Sources and references

- 5.1. Data Protection Act 2018,
- 5.2. UK General Data Protection Regulation 2016 (UKGDPR).

6. Other useful documents

- 6.1. Subject Access Request Policy
- 6.2. Freedom of Information Policy
- 6.3. Privacy Notice Policy
- 6.4. Equality Policy
- 6.5. Publication Scheme
- 6.6. Complaints Policy
- 6.7. Data Protection Policy

7. Monitoring

- 7.1. This policy will be monitored through the MAT's accountability framework.
- 7.2. An assessment of compliance with requirements will be undertaken in order to provide:
 - 7.2.1. Assurance
 - 7.2.2. Gap analysis of policy and practice
 - 7.2.3. Examples of best practice
 - 7.2.4. Improvement and training plans
- 7.3. Reports will be submitted to the Governing Body / Trust Board.

