NEW BRIDGE
MULTI ACADEMY TRUST

Data Protection Policy

Document Control Information	
Document Title	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	10th June 2015	Trustees	10/06/2017
R Righini	Policy review and extraction of sections into separate policies	2	31st August 2017	Trustees	31.08/2019
R Righini	Policy review re new GDPR rules	3	28th 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 exit	5	01/12/2022	n/a	30/11/2024

Equality Impact

Statement 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.

The person responsible for equality impact assessment for this document is the Director of Equality and Diversity.

Screening This document has been screened by the Equality Team and the impact has been assessed as:

- ☐ Not applicable
- ☐ Low
- ☐ Medium
- ☐ High

Equality Impact Assessment Form

To be completed by document author / lead person

Title of document		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	**Medium Impact**	**Low Impact**
The policy or process has a major impact on equality	The policy or process has an impact on equality	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 integrity, availability, and 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.

   1.2. This policy sets out the key data protection obligations and accountability to which we are fully committed.

2. **Scope of Policy**

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

   2.1.1. members of the public (adults and children)
   2.1.2. current, past, prospective employees
   2.1.3. clients and customers
   2.1.4. contractors and suppliers
   2.1.5. elected members

   2.2. This policy covers all aspects of handling personal data, regardless of 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 compliant with data protection legislation, particularly the Data Protection Act 2018 and the UK General Data Protection Regulation 2016 (UKGDPR).

   2.4. This policy meets the requirements of the Protection of Freedoms Act 2012 when referring to our use of biometric data.

   2.5. This policy reflects the ICO's code of practice for the use of surveillance cameras and personal information.

   2.6. This policy complies with regulation 5 of the Education (Pupil Information) (England) Regulations 2005, which gives parents the right of access to their child's educational record.

   2.7. This policy reflects the commitment to be compliant with data protection legislation, particularly the Data Protection Act 2018, the UK General Data Protection Regulation 2016 (UKGDPR).

3. **Reason for Review**
   3.1. This policy was reviewed in line with new GDPR regulations following EU exit.

4. **Aim(s)**
   4.1. 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.

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 data subject enquiries and communications with the Information Commissioner's Office.
   5.1.1. Data Protection Officer on behalf of New Bridge Multi Academy Trust:

Justin Hardy
West Street
Oldham
OL1 1UT

Email: DPO@oldham.gov.uk

5.2. Definitions of personal data:

5.2.1. ***Personal data*** means any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person;

In summary, anything and everything that can relate to a living person.

5.2.2. ***Special Personal data*** means personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade-union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation

In summary, these are the data categories that are subject to additional controls in order to prevent unauthorised collection, use, access etc.

5.2.3. ***Crime data*** means criminal offence data, e.g., alleged commission of offences or proceedings for an offence, (actual or alleged), including sentencing, (other than where it is **USED** for Law Enforcement (LED) functions) by competent authorities within the scope of Part 3 of the Data Protection Act 2018. In other words, statutory functions of the local authority for the purposes of the prevention, investigation, detection or prosecution of criminal offences, the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security.

In summary this type of personal data is subject to specific conditions and controls.

5.3. **Data Protection Principles**: There are six principles which provide the framework for personal data handling and for which the council is accountable for compliance. Personal data shall be:

5.3.1. *(a) processed lawfully, fairly and in a transparent manner*
To be lawful an appropriate condition of processing needs to be identified. To be fair and transparent a privacy notice needs to be provided/made available to the data subject whose personal data is being handled and the law specifies what information must be communicated.

5.3.2. *(b) processed for an explicit and specific purpose and not processed for other incompatible purposes. Scientific/historical/statistical research is not incompatible and nor is archiving in the public interest*
Personal data should only be used for the stated lawful purposes, except where the law permits.

5.3.3. *(c) adequate, relevant and limited to what is necessary for the purpose*
Ensure that personal data is specific to the stated lawful purpose and is not excessive or unnecessary.

5.3.4. *(d) accurate and, where necessary, kept up to date; ensuring that personal data that are inaccurate, are erased or rectified without delay.*
Ensure that personal data is correct and that any errors are rectified and where appropriate notified to recipients of the personal data.

5.3.5. *(e) keep no longer than necessary for the purpose, but can keep for longer is solely for Scientific/historical/statistical research and archiving in the public interest purposes and is kept securely*
Personal data should not be kept longer than necessary, taking into account any legal and operational requirements.

5.3.6. *(f) protection of the personal data using appropriate technical or organisational measures.*
These measures should be selected on the basis of identified threats and risks to personal data and the potential impact on the data subjects, the council and any third parties who are sources, recipients, or processors of the personal data.

5.4. **Mandatory obligations**: we will ensure that we are appropriately registered with the Information Commissioner's Office (ICO) and create and maintain the mandatory Record of Processing Activities (ROPA), to be made available to the (ICO) upon demand

5.5. **Data Protection Impact Assessments (DPIA)**: are an important tool in ensuring that we integrate data protection by design by default into our technical systems and day to day business operations. This can be done by embedding privacy risk considerations into new (and / or changes to) systems and business processes. A DPIA must take place where it is identified that 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 the recommendations of the DPO are not being considered the Headteacher must approve any acceptance of these risks. Where risks are high and not adequately mitigated a referral to the Information Commissioner's Office (ICO) must be made.

5.6. **Data Collection, use and disclosure**: We handle personal data that has been either collected from the data subject and/or other parties, e.g. other people, public sector and regulatory organisations, private and voluntary sector organisations etc. We will:

5.6.1. only handle personal data where there is a legal basis to do so.

5.6.2. not unnecessarily rely on consent where an alternative legal basis is available for processing personal data. However, where consent/explicit consent, is the lawful basis, then we acknowledge that for consent to be valid it must be freely given and capable of being withdrawn. Where a particular individual is unable, due to age, capacity or other reasons, to give consent directly, consent will be sought from an appropriate person e.g., parent, guardian, legal representative etc.

5.6.3. provide data subjects with privacy notices that explain how their personal data will be processed and how to exercise their individual data rights

5.6.4. in the event of a personal data security breach, resulting in a high risk to the data subject(s), to notify the data subjects and / or the ICO as appropriate.

5.6.5. in the event of a data subject exercising their individual data rights, we will assess the request and respond within the statutory timeline and provide a complaints process and Individual Rights Policy.

5.6.6. If we offer online services to pupils, such as classroom apps, and we intend to rely on consent as a basis for processing, we will get parental consent where the pupil is under 13 (except for online counselling and preventive services).

5.6.7. We will obtain written consent from parents/carers or pupils aged 18 or over for photographs/videos of children to be used for communication/publicity/marketing materials.

5.6.8. Where we use pupils and/or staffs biometric recognition data eg, cashless school dinners, consent from parents/carers and staff will be sought in advance. An alternative system will be provided for those people who do not wish to participate or later withdraw consent.

5.6.9. We use CCTV in various locations around our trust sites to ensure they remain safe. We do not need to ask individuals' permission to use CCTV, but we make it clear where individuals are being recorded. Security cameras are clearly visible and accompanied by prominent signs explaining that CCTV is in use. Any enquiries about the CCTV system should be directed to the Director of Estates.

5.6.10. ensure personal data is subject to appropriate retention and security controls taking into account the nature of the data and the information risks. Personal data may be stored for longer periods where it is for archiving in the public interest, historical or scientific research purposes, or as required by legislation or regulatory activity.

5.6.11. ensure that when sharing and disclosing personal data this is undertaken within the parameters of the law to prevent 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 where appropriate a 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.

5.6.12. when handling health and social care personal data, that the Caldicott Principles and National Data Guardian Standards are observed. If any processing falls within the scope of the national data opt-out we follow the prescribed processed to check if any data subjects have opted out of their data being used for this purpose.

5.6.13. when handling special category, crime conviction and offence data, that we comply with the additional policy requirements necessary to support these particular processing activities in order to demonstrate compliance with the data protection principles and retention policies and ensure inclusion in the Records of Processing Activities (ROPA).

5.6.14. ensure 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 as data controller.

5.6.15. not transfer 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.

5.6.16. provide all staff and governors / trustees with data protection training as part of their induction process. Data protection will also form part of continuing professional development, where changes to legislation, guidance or the trust's processes make it necessary.

5.6.17. to co-operate and provide information to the ICO and other regulatory bodies in pursuance of any investigation or enforcement action.

5.7. **Offences**: The data protection legislation contains specific offences:

5.7.1. It is an offence for a person knowingly or recklessly, without the consent of the data controller, to:

5.7.1.1. obtain or disclose personal data
5.7.1.2. procure the disclosure of personal data to another person
5.7.1.3. retain it without the consent of the original data controller
5.7.1.4. offer to sell or buy the personal data obtained

5.7.2. It is an offence for 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.

5.7.3. It is an offence 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.

5.7.4. It is an offence 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.

5.7.5. It is an offence to intentionally obstruct or give false information to the ICO in the exercise of its powers under information notices and/or warrants.

6. **Sources and references**
   6.1. Data Protection Act 2018,
   6.2. UK General Data Protection Regulation 2016 (UKGDPR).
   6.3. Protection of Freedoms Act 2012
   6.4. Education (Pupil Information) (England) Regulations 2005

7. **Other useful documents**
   7.1. This policy must be read alongside the following supporting policies:
      7.1.1. Individual Rights Policy
      7.1.2. Data Subject Access Policy
      7.1.3. DPIA Policy
      7.1.4. Personal Data Sharing Policy
      7.1.5. Special and Crime Personal Data Policy

8. **Monitoring**
   8.1. This policy will be monitored through the MAT's accountability framework in order to provide
      8.1.1. Assurance
      8.1.2. Gap analysis of policy and practice
      8.1.3. Examples of best practice
      8.1.4. Improvement and training plans