New Bridge Multi Academy Trust Schools

Hollinwood Academy, Hawthorns School, New Bridge School, Samuel Laycock, Springboard Project, Spring Brook Academy

Special Personal Data

Additional Data Protection Policy

Version 3

February 2023

1. Objectives

1.1. 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.

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

- General processing
- 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)

2. Scope

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:

- racial or ethnic origin;
- religious or philosophical beliefs;
- political opinions or trade-union membership;
- the processing of genetic data or biometric data for the purpose of uniquely identifying a natural person;
- data concerning health
- a person's sexual life or sexual orientation
- criminal conviction or offence data

2.3. 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.

2.4. 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.

2.5. This policy reflects the commitment to data protection compliance and the privacy elements of human rights legislation. In particular this includes:

- the UK General Data Protection Regulation 2016 (UKGDPR) as supplemented by the Data Protection Act 2018 (DPA 2018)
- Protection of Freedoms Act 2012 (PFA 2012)
- the UK Human Rights Act 1998.

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 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 [school name]
West Street
Oldham
OL1 1UT

Email: DPO@oldham.gov.uk

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

3.2.1. (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.

3.2.2. (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.

3.2.3. (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.

3.2.4. (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.

3.2.5. (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.

3.2.6. (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.

3.3. **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.

3.4. **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.

3.5. **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.

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

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

3.6.2. With the exception of biometric data of pupils, 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.

3.6.3. Seeking consent for the use of biometric data of pupils in accordance with the PFA 2012. To ensure that this consent meets the requirements of UKGDPR and in accordance with the PFA 2012, reasonable alternative arrangements must be provided for pupils where consent has not been given or has been withdrawn/overridden. More information relating to the use of biometric data of children can be found in Annex A.

3.6.4. Only sending promotional or marketing material with consent/or existing business relationship.

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

3.6.6. 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.

3.6.7. Assisting individuals to exercise their personal data rights, and to responding within the statutory time limits and providing a complaints process.

3.6.8. 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.

3.6.9. 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.

3.6.10. Ensuring our Records of Processing Activities (RoPA) are maintained

3.6.11. 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.

3.6.12. 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.

3.6.13. Co-operating and providing information to the ICO and other regulatory bodies in pursuance of any investigation or enforcement action.

3.7. **Offences**: The data protection legislation contains specific offences. It is an offence:

3.7.1. For a person knowingly or recklessly, without the consent of the data controller to

- obtain or disclose personal data
- procure the disclosure of personal data to another person
- retain it without the consent of the original data controller
- offer to sell, sell or buy the personal data obtained

3.7.2. 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.

3.7.3. 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.

3.7.4. 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.

3.7.5. To intentionally obstruct or give false information to the ICO in the exercise of its powers under information notices and/or warrants.

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

4.2. Reports will be submitted to the Governing Body / Trust Board.

5. Authority for this policy

5.1. The Governing Body / Trust Board has overall responsibility for ensuring that our school complies with all relevant data protection obligations.

5.2. 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. The Data Protection Officer (DPO) 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.

Annex A - Biometric data of children in schools

What is Biometric Data?

Biometric data means personal information resulting from specific technical processing relating to the individual's physical, psychological or behavioural characteristics which allow or confirm the unique identification of that person, such as facial images, voice recognition or fingerprints.

Who can give consent?

In order to comply with the requirements of the Protection of Freedoms Act 2012 (PFA 2012), we understand that we must notify each parent, carer/legal guardian of the child of our intention to process the child's biometric information, and that the parent may object at any time to the processing of the information.

We will ensure that a child's biometric information will not be processed unless at least one parent of the child consents, and no parent of the child has withdrawn his or her consent, or otherwise objected, to the information being processed. In addition, a pupil's or student's objection or refusal, overrides any parental consent to the processing, therefore any biometric data will not be processed.

The PFA 2012 defines a parent to mean "a parent of the child and any individual who is not a parent of the child but who has parental responsibility for the child". Practically it would be person(s) with parental responsibility for the child, be it birth, adoptive or an appointed body, who a school or college would notify and seek consent from to process personal biometric data. Any one parent could give or withhold consent.

Where a child is looked after and is subject to a care order in favour of the local authority or the local authority provides accommodation for the child within the definition of section 22(1) of the Children Act 1989, we will not be required to notify or seek consent from birth parents.

Pupils' and students' right to refuse

If a pupil under 18 objects or refuses to participate (or to continue to participate) in activities that involve the processing of their biometric data, we will ensure that the pupil's biometric data is not taken/used as part of a biometric recognition system. A pupil's objection or refusal overrides any parental consent to the processing. Section 26 and Section 27 of the PFA 2012 makes no reference to a lower age limit in terms of a child's right to refuse to participate in sharing their biometric data.

We will take appropriate steps to ensure that pupils understand that they can object or refuse to allow their biometric data to be taken/used and that, if they do this, we will provide them with an alternative method of accessing relevant services. The steps taken to inform pupils and students should take account of their age and level of understanding.

Parents should also be told of their child's right to object or refuse and be encouraged to discuss this with their child.

Once a student is 18 years old they will be considered an adult and as such parental consent is no longer relevant.

Provision of Alternative Arrangements

Reasonable alternative arrangements must be provided for pupils who do not use automated biometric recognition systems either because their parents have refused consent (or a parent has objected in writing) or due to the pupil's own refusal to participate in the collection of their biometric data.

The alternative arrangements should ensure that pupils do not suffer any disadvantage or difficulty in accessing services/premises etc. as a result of their not participating in an automated biometric recognition system. Likewise, such arrangements should not place any additional burden on parents whose children are not participating in such a system.