GDPR Data Protection Policy

May 2018

Contents:

Statement of intent

Blackpool Multi Academy Trust is required to keep and process certain information about its staff members and pupils in accordance with its legal obligations under the General Data Protection Regulation (GDPR) and Data Protection Act 2018.

The Trust may, from time to time, be required to share personal information about its staff or pupils with other organisations, mainly the LA, other Trusts and educational bodies, and potentially social services.

This policy is in place to ensure all staff and governors are aware of their responsibilities and outlines how the Trust complies with the following core principles of the GDPR.

Organisational methods for keeping data secure are imperative, and **Blackpool Multi Academy Trust** believes that it is good practice to keep clear practical policies, backed up by written procedures.

This policy complies with the requirements set out in the GDPR, which came into effect on 25 May 2018.

Signed by:

_____ Executive Leader Date: _____

_____ Chair of governors Date: _____

1. Legal framework

1.1. This policy has due regard to legislation, including, but not limited to the following:

- The General Data Protection Regulation (GDPR)
- Data Protection Act 2018
- The Freedom of Information Act 2000
- The Education (Pupil Information) (England) Regulations 2005 (as amended in 2016)
- The Freedom of Information Act 2000 and Data Protection (Appropriate Limit and Fees) Regulations 2004
- The Trust Standards and Framework Act 1998

1.2. This policy will also have regard to the following guidance:

- Information Commissioner's Office 'Overview of the General Data Protection Regulation (GDPR)'

1.3. This policy will be implemented in conjunction with the following other Trust policies:

- **Compliant Records Management Policy**
- **Data Breach Policy**
- **CCTV Policy**

2. Applicable data

2.1. For the purpose of this policy, **personal data** refers to information that relates to an identifiable, living individual, including information such as an online identifier, such as an IP address. The GDPR applies to both automated personal data and to manual filing systems, where personal data is accessible according to specific criteria, as well as to chronologically ordered data and pseudonymised data, e.g. key-coded.

2.2. **Sensitive personal data** is referred to in the GDPR as 'special categories of personal data', which are broadly the same as those in the Data Protection Act (DPA) 1998. These include race, ethnic religion, politics, religion, trade union membership, genetics, biometrics, health, sex life or sexual orientation.

3. Principles

3.1. In accordance with the requirements outlined in the GDPR, personal data will be:

- Processed lawfully, fairly and in a transparent manner in relation to individuals.
- Collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall not be considered to be incompatible with the initial purposes.
- Adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed.
- Accurate and, where necessary, kept up-to-date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay.
- Kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods, insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes, subject to implementation of the appropriate technical and organisational measures required by the GDPR in order to safeguard the rights and freedoms of individuals.
- Processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.

3.2. The GDPR also requires that "the controller shall be responsible for, and able to demonstrate, compliance with the principles".

4. Accountability

4.1. **Blackpool Multi Academy Trust** will implement appropriate technical and organisational measures to demonstrate that data is processed in line with the principles set out in the GDPR.

4.2. The Trust will provide comprehensive, clear and transparent privacy policies.

4.3. Records of activities relating to higher risk processing will be maintained, such as the processing of special categories data or that in relation to criminal convictions and offences.

4.4. When the Trust uses a processor, it will have a written contract in place. This is important so that both parties understand their responsibilities and liabilities.

5. Data protection officer (DPO)

5.1. A DPO has been appointed in order to:

- Inform and advise the Trust and its employees about their obligations to comply with the GDPR and other data protection laws.
- Monitor the Trust's compliance with the GDPR and other laws, including managing internal data protection activities, advising on data protection impact assessments, conducting internal audits, and providing the required training to staff members.

5.2. The DPO's contact details are as follows:

Data Protection Officer, Blackpool Council

Blackpool Council, Number One, Bickerstaffe Square, Blackpool, FY1 3AH

SchoolsDPO@blackpool.gov.uk

6. Lawful processing

6.1. The legal basis for processing data will be identified and documented prior to data being processed.

6.2. Under the GDPR, data will be lawfully processed under the following conditions:

- The consent of the data subject has been obtained.
- Processing is necessary for:
  - Compliance with a legal obligation.
  - The performance of a task carried out in the public interest or in the exercise of official authority vested in the controller.
  - For the performance of a contract with the data subject or to take steps to enter into a contract.
  - Protecting the vital interests of a data subject or another person.
  - For the purposes of legitimate interests pursued by the controller or a third party, except where such interests are overridden by the interests, rights or freedoms of the data subject.

6.3. Sensitive data will only be processed under the following conditions:

- Explicit consent of the data subject, unless reliance on consent is prohibited by EU or Member State law.
- Processing carried out by a not-for-profit body with a political, philosophical, religious or trade union aim provided the processing relates only to members or former members (or those who have regular contact with it in connection with those purposes) and provided there is no disclosure to a third party without consent.
- Processing relates to personal data manifestly made public by the data subject.

- Processing is necessary for:
    - Carrying out obligations under employment, social security or social protection law, or a collective agreement.
    - Protecting the vital interests of a data subject or another individual where the data subject is physically or legally incapable of giving consent.
    - The establishment, exercise or defence of legal claims or where courts are acting in their judicial capacity.
    - Reasons of substantial public interest on the basis of Union or Member State law which is proportionate to the aim pursued and which contains appropriate safeguards.
    - The purposes of preventative or occupational medicine, for assessing the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment or management of health or social care systems and services on the basis of Union or Member State law or a contract with a health professional.
    - Reasons of public interest in the area of public health, such as protecting against serious cross-border threats to health or ensuring high standards of healthcare and of medicinal products or medical devices.
    - Archiving purposes in the public interest, or scientific and historical research purposes or statistical purposes in accordance with Article 89(1).

7. Consent

7.1. Consent must be a positive indication. It cannot be inferred from silence, inactivity or pre-ticked boxes.

7.2. Consent will only be accepted where it is freely given, specific, informed and an unambiguous indication of the individual's wishes.

7.3. Where consent is given, a record will be kept documenting how and when consent was given.

7.4. The Trust ensures that consent mechanisms meet the standards of the GDPR. Where the standard of consent cannot be met, an alternative legal basis for processing the data must be found, or the processing must cease.

7.5. Consent accepted under the DPA will be reviewed to ensure it meets the standards of the GDPR; however, acceptable consent obtained under the DPA 1998 will not be reobtained.

7.6. Consent can be withdrawn by the individual at any time.

8. The right to be informed

8.1. The privacy notice supplied to individuals in regards to the processing of their personal data will be written in clear, plain language which is concise, transparent, easily accessible and free of charge.

8.2. If services are offered directly to a child, the Trust will ensure that the privacy notice is written in a clear, plain manner that the child will understand.

8.3. For data obtained directly from the data subject, this information will be supplied at the time the data is obtained.

8.4. In relation to data that is not obtained directly from the data subject, this information will be supplied:

- Within one month of having obtained the data.
- If disclosure to another recipient is envisaged, at the latest, before the data are disclosed.
- If the data are used to communicate with the individual, at the latest, when the first communication takes place.

9. The right of access

9.1. Individuals have the right to obtain confirmation that their data is being processed.

9.2. Individuals have the right to submit a subject access request (SAR) to gain access to their personal data in order to verify the lawfulness of the processing.

9.3. The Trust will verify the identity of the person making the request before any information is supplied.

9.4. A copy of the information will be supplied to the individual free of charge; however, the Trust may impose a 'reasonable fee' to comply with requests for further copies of the same information or where a where a request is manifestly unfounded, excessive or repetitive, a reasonable fee will be charged.

9.5. All requests will be responded to without delay and at the latest, within one month of receipt.

9.6. In the event of numerous or complex requests, the period of compliance will be extended by a further two months. The individual will be informed of this extension, and will receive an explanation of why the extension is necessary, within one month of the receipt of the request.

9.7. In the event that a large quantity of information is being processed about an individual, the Trust will ask the individual to specify the information the request is in relation to.

9.8. If individuals wish to submit a request in writing they can do so by writing to the school or emailing ***insert email address.***

10. Remaining individual rights

10.1. Individuals also have six other rights under the GDPR which are as follows:

- Right to rectification - individuals are entitled to have any inaccurate or incomplete personal data rectified.
- Right to erasure - individuals hold the right to request the deletion or removal of personal data where there is no compelling reason for its continued processing.
- Right to restrict processing - individuals have the right to block or suppress the Trust's processing of personal data.
- Right to data portability - Individuals have the right to obtain and reuse their personal data for their own purposes across different services.
- Right to object – individuals have the right to object to the processing of their personal data in certain circumstances.
- Rights in relation to automated decisions and profiling

10.2. If individuals wish to submit a request in writing they can do so by writing to the school or emailing ***insert email address.***

10.3. On receipt of a request, the Trust will seek the advice of its DPO who will carefully consider each request on a case by case basis.

11. Privacy by design and privacy impact assessments

11.1. The Trust will act in accordance with the GDPR by adopting a privacy by design approach and implementing technical and organisational measures which demonstrate how the Trust has considered and integrated data protection into processing activities.

11.2. Data protection impact assessments (DPIAs) will be used to identify the most effective method of complying with the Trust's data protection obligations and meeting individuals' expectations of privacy.

11.3. DPIAs will allow the Trust to identify and resolve problems at an early stage, thus reducing associated costs and preventing damage from being caused to **Blackpool Multi Academy Trust** reputation which might otherwise occur.

11.4. A DPIA will be used when using new technologies or when the processing is likely to result in a high risk to the rights and freedoms of individuals.

11.5. Where a DPIA indicates high risk data processing, the Trust will consult the ICO to seek its opinion as to whether the processing operation complies with the GDPR.

12. Data breaches

12.1. The term 'personal data breach' refers to a breach of security which has led to the destruction, loss, alteration, unauthorised disclosure of, or access to, personal data.

12.2. The **Executive Leader** will ensure that all staff members are made aware of, and understand, what constitutes as a data breach as part of their continuous development training.

12.3. Where a breach is likely to result in a risk to the rights and freedoms of individuals, the relevant supervisory authority will be informed.

12.4. All notifiable breaches will be reported to the relevant supervisory authority within 72 hours of the Trust becoming aware of it.

12.5. The risk of the breach having a detrimental effect on the individual, and the need to notify the relevant supervisory authority, will be assessed on a case-by-case basis by Trust's DPO.

12.6. In the event that a breach is likely to result in a high risk to the rights and freedoms of an individual, the Trust will notify those concerned directly.

12.7. Effective and robust breach detection, investigation and internal reporting procedures are in place at the Trust, which facilitate decision-making in relation to whether the relevant supervisory authority or the public need to be notified.

13. Data security

13.1. Confidential paper records will be kept in a locked filing cabinet, drawer or safe, with restricted access.

13.2. Confidential paper records will not be left unattended or in clear view anywhere with general access.

13.3. Digital data is coded, encrypted or password-protected, both on a local hard drive and on a network drive that is regularly backed up off-site.

13.4. Where data is saved on removable storage or a portable device, the device will be kept in a locked filing cabinet, drawer or safe when not in use.

13.5. Memory sticks will not be used to hold personal information unless they are password-protected and fully encrypted.

13.6. All electronic devices are password-protected to protect the information on the device in case of theft.

13.7. Where possible, the Trust enables electronic devices to allow the remote blocking or deletion of data in case of theft.

13.8. Staff and governors will not use their personal laptops or computers for Trust purposes.

13.9. All necessary members of staff are provided with their own secure login and password, and every computer regularly prompts users to change their password.

13.10. Emails containing sensitive or confidential information are password-protected if there are unsecure servers between the sender and the recipient.

13.11. Circular emails to parents are sent blind carbon copy (bcc), so email addresses are not disclosed to other recipients.

13.12. When sending confidential information by fax, staff will always check that the recipient is correct before sending.

13.13. Where personal information that could be considered private or confidential is taken off the premises, either in electronic or paper format, staff will take extra care to follow the same procedures for security, e.g. keeping devices under lock and key. The person taking the information from the Trust premises accepts full responsibility for the security of the data.

13.14. Before sharing data, all staff members will ensure:

- They are allowed to share it.
- That adequate security is in place to protect it.
- Who will receive the data has been outlined in a privacy notice.

13.15. Under no circumstances are visitors allowed access to confidential or personal information. Visitors to areas of the Trust containing sensitive information are supervised at all times.

13.16. The physical security of the Trust's buildings and storage systems, and access to them, is reviewed on a **termly** basis. If an increased risk in vandalism/burglary/theft is identified, extra measures to secure data storage will be put in place.

13.17. **Blackpool Multi Academy Trust** takes its duties under the GDPR seriously and any unauthorised disclosure may result in disciplinary action.

14. CCTV and photography

14.1. The Trust understands that recording images of identifiable individuals constitutes as processing personal information, so it is done in line with data protection principles.

14.2. The Trust notifies all pupils, staff and visitors of the purpose for collecting CCTV images via notice boards, letters and email.

14.3. Cameras are only placed where they do not intrude on anyone's privacy and are necessary to fulfil their purpose.

14.4. All CCTV footage will be kept in line with each individual Academy's CCTV policy for security purposes for (up to a maximum of 3 months).

14.5. The Trust will always indicate its intentions for taking photographs of pupils and will retrieve permission before publishing them.

14.6. If the Trust wishes to use images/video footage of pupils in a publication, such as the Trust website, prospectus, or recordings of Trust plays, written permission will be sought for the particular usage from the parent of the pupil.

14.7. Images captured by individuals for recreational/personal purposes, and videos made by parents for family use, are exempt from the GDPR.

15. Data retention

15.1. Data will not be kept for longer than is necessary in line with the Trusts Record Management Policy.

15.2. Unrequired data will be deleted as soon as practicable.

15.3. Some educational records relating to former pupils or employees of the Trust may be kept for an extended period for legal reasons, but also to enable the provision of references or academic transcripts.

15.4. Paper documents will be shredded or pulped, and electronic memories scrubbed clean or destroyed, once the data should no longer be retained.

16. Policy review

16.1. This policy is reviewed every **two years** by the **Data Protection Officer** and the **Executive Leader.**

The next scheduled review date for this policy is **May 2020.**