Leeds Diocesan Learning Trust (LDLT)

Company Number 13687278

GDPR Policy

Data Protection and Personal Data

1.1. GDPR Data protection policy

1. Data Protection Policy

1.1. Importance of Data Protection

In order to operate as an organisation we hold Personal Data about employees, suppliers, examination invigilators, volunteers, pupils and their family members, and carers and other individuals. The use of Personal Data is governed by the General Data Protection Regulation (the "**GDPR**"). We take data protection very seriously and understand the impact that data breaches and misuse of data may have on data subjects as well as on our activities. Compliance with this policy is necessary for us to maintain the confidence and trust of those whose Personal Data we handle.

Non-compliance with this policy by employees could in certain circumstances constitute a serious disciplinary matter. Training (including refresher training) is provided at induction and on a periodic basis. Staff and Volunteers are expected to maintain their knowledge and appreciation of data protection law and this will be supported by the organisation through, in particular, regular access to training. Please contact the Data Protection Officer if you feel that you require access to that course at any point. From time to time the Trust will require the successful completion of data protection training courses.

The operation of this Policy will be monitored by the Data Protection Officer who shall ensure that it is kept up to date. If you have any questions concerning this Framework or believe that it can be improved in any respect please discuss with the Data Protection Officer.

This Policy Statement

The aim of this Policy is to give you a basic understanding of the data protection laws, our responsibility in respect of data protection practice, your rights and obligations and to explain why privacy is so important to us. It applies to all actions we take which involve the processing of and working with Personal Data.

The 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).

The Academy may, from time to time, be required to share personal information about its staff or pupils with other organisations, mainly the LA, other schools and educational bodies, and potentially children's services.

This policy complies with the requirements set out in the GDPR, which came into effect on 25 May 2018. The government have confirmed that the UK's decision to leave the EU will not affect the commencement of the GDPR.

2. Legal framework

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

- The Data Protection Act 2018
- The General Data Protection Regulation (GDPR)
- The Freedom of Information Act 2000
- The Education (Pupil Information) (England) Regulations 2005 (as amended in 2016)

- The Freedom of Information and Data Protection (Appropriate Limit and Fees) Regulations 2004
- The School Standards and Framework Act 1998

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

- Information Commissioner's Office (2017) 'Overview of the General Data Protection Regulation (GDPR)'
- Information Commissioner's Office (2017) 'Preparing for the General Data Protection Regulation (GDPR) 12 steps to take now'

2.3. This policy will be implemented in conjunction with the following other school policies:

- E-security Policy
- Freedom of Information Policy
- CCTV Policy

3. Applicable data

3.1. 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, e.g. 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.

3.2. **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 specifically include the processing of genetic data, biometric data and data concerning health matters.

4. Principles

4.1. 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.

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

5. Accountability

5.1. The Trust will implement appropriate technical and organisational measures to demonstrate that data is processed in line with the principles set out in the GDPR.

5.2. The Academy will provide comprehensive, clear and transparent privacy policies.

5.3. 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.

5.4. Internal records of processing activities will include the following:

- Name and details of the organisation
- Purpose(s) of the processing
- Description of the categories of individuals and personal data
- Retention schedules
- Categories of recipients of personal data
- Description of technical and organisational security measures
- Details of transfers to third countries, including documentation of the transfer mechanism safeguards in place

5.5. The Academy will implement measures that meet the principles of data protection by design and data protection by default, such as:

- Data minimisation.
- Pseudonymisation.
- Transparency.
- Allowing individuals to monitor processing.
- Continuously creating and improving security features.

5.6. Data protection impact assessments will be used, where appropriate.

6. Data protection officer (DPO)

6.1. A DPO will be appointed in order to:

- Inform and advise the Academy and its employees about their obligations to comply with the GDPR and other data protection laws.

- Monitor the Academy'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.

6.2. An existing employee of the Trust has been appointed to the role of DPO. The current DPO is the Chief Financial Officer to the Trust. Each school will have an individual who is responsible for data protection within the school (nominated person).

6.3. The individual appointed as DPO will have professional experience and knowledge of data protection law.

6.4. The DPO will report to the CEO. The nominated person will report to the highest level of management at the school, which is the **Headteacher**.

6.5. The DPO will operate independently and will not be dismissed or penalised for performing their duties.

7. Lawful processing

7.1. The legal basis for processing data has been identified and documented prior to data being processed.

7.2. 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. (This condition is not available to processing undertaken by the Academy in the performance of its tasks.)

7.3. 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).

8. Consent

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

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

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

8.4. The Academy 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.

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

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

8.7. Where a child is under the age of **13** the consent of parents will be sought prior to the processing of their data, except where the processing is related to preventative or counselling services offered directly to a child.

9. The right to be informed

9.1. 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.

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

9.3. In relation to data obtained both directly from the data subject and not obtained directly from the data subject, the following information will be supplied within the privacy notice:

- The identity and contact details of the controller (and where applicable, the controller's representative) and the DPO.
- The purpose of, and the legal basis for, processing the data.
- The legitimate interests of the controller or third party.
- Any recipient or categories of recipients of the personal data.
- Details of transfers to third countries and the safeguards in place.
- The retention period of criteria used to determine the retention period.
- The existence of the data subject's rights, including the right to:
  - Withdraw consent at any time.
  - Lodge a complaint with a supervisory authority.
- The existence of automated decision making, including profiling, how decisions are made, the significance of the process and the consequences.

9.4. Where data is obtained directly from the data subject, information regarding whether the provision of personal data is part of a statutory or contractual requirement, as well as any possible consequences of failing to provide the personal data, will be provided.

9.5. Where data is not obtained directly from the data subject, information regarding the categories of personal data that the Academy holds, the source that the personal data originates from and whether it came from publicly accessible sources, will be provided.

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

9.7. 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.

10. The right of access

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

10.2. 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.

10.3. The Academy will verify the identity of the person making the request before any information is supplied.

10.4. A copy of the information will be supplied to the individual free of charge; however, the Academy may impose a 'reasonable fee' to comply with requests for further copies of the same information.

10.5. Where a SAR has been made electronically, the information will be provided in a commonly used electronic format.

10.6. Where a request is manifestly unfounded, excessive or repetitive, a reasonable fee will be charged.

10.7. All fees will be based on the administrative cost of providing the information.

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

10.9. 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.

10.10. Where a request is manifestly unfounded or excessive, the Academy holds the right to refuse to respond to the request. The individual will be informed of this decision and the reasoning behind it, as well as their right to complain to the supervisory authority and to a judicial remedy, within one month of the refusal.

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

11. The right to rectification

11.1. Individuals are entitled to have any inaccurate or incomplete personal data rectified.

11.2. Where the personal data in question has been disclosed to third parties, the Academy will inform them of the rectification where possible.

11.3. Where appropriate, the Academy will inform the individual about the third parties that the data has been disclosed to.

11.4. Requests for rectification will be responded to within one month; this will be extended by two months where the request for rectification is complex.

11.5. Where no action is being taken in response to a request for rectification, the Academy will explain the reason for this to the individual, and will inform them of their right to complain to the supervisory authority and to a judicial remedy.

12. The right to erasure

12.1. Individuals hold the right to request the deletion or removal of personal data where there is no compelling reason for its continued processing.

12.2. Individuals have the right to erasure in the following circumstances:

- Where the personal data is no longer necessary in relation to the purpose for which it was originally collected/processed
- When the individual withdraws their consent
- When the individual objects to the processing and there is no overriding legitimate interest for continuing the processing
- The personal data was unlawfully processed
- The personal data is required to be erased in order to comply with a legal obligation

- The personal data is processed in relation to the offer of information society services to a child

12.3. The Academy has the right to refuse a request for erasure where the personal data is being processed for the following reasons:

- To exercise the right of freedom of expression and information
- To comply with a legal obligation for the performance of a public interest task or exercise of official authority
- For public health purposes in the public interest
- For archiving purposes in the public interest, scientific research, historical research or statistical purposes
- The exercise or defence of legal claims

12.4. As a child may not fully understand the risks involved in the processing of data when consent is obtained, special attention will be given to existing situations where a child has given consent to processing and they later request erasure of the data, regardless of age at the time of the request.

12.5. Where personal data has been disclosed to third parties, they will be informed about the erasure of the personal data, unless it is impossible or involves disproportionate effort to do so.

12.6. Where personal data has been made public within an online environment, the Academy will inform other organisations who process the personal data to erase links to and copies of the personal data in question.

13. The right to restrict processing

13.1. Individuals have the right to block or suppress the Academy's processing of personal data.

13.2. In the event that processing is restricted, the Academy will store the personal data, but not further process it, guaranteeing that just enough information about the individual has been retained to ensure that the restriction is respected in future.

13.3. The Academy will restrict the processing of personal data in the following circumstances:

- Where an individual contests the accuracy of the personal data, processing will be restricted until the Academy has verified the accuracy of the data
- Where an individual has objected to the processing and the Academy is considering whether their legitimate grounds override those of the individual
- Where processing is unlawful and the individual opposes erasure and requests restriction instead
- Where the Academy no longer needs the personal data but the individual requires the data to establish, exercise or defend a legal claim

13.4. If the personal data in question has been disclosed to third parties, the Academy will inform them about the restriction on the processing of the personal data, unless it is impossible or involves disproportionate effort to do so.

13.5. The Academy will inform individuals when a restriction on processing has been lifted.

14. The right to data portability

14.1. Individuals have the right to obtain and reuse their personal data for their own purposes across different services.

14.2. Personal data can be easily moved, copied or transferred from one IT environment to another in a safe and secure manner, without hindrance to usability.

14.3. The right to data portability only applies in the following cases:

- To personal data that an individual has provided to a controller
- Where the processing is based on the individual's consent or for the performance of a contract
- When processing is carried out by automated means

14.4. Personal data will be provided in a structured, commonly used and machine-readable form.

14.5. The Academy will provide the information free of charge.

14.6. Where feasible, data will be transmitted directly to another organisation at the request of the individual.

14.7. The Academy is not required to adopt or maintain processing systems which are technically compatible with other organisations.

14.8. In the event that the personal data concerns more than one individual, the Academy will consider whether providing the information would prejudice the rights of any other individual.

14.9. The Academy will respond to any requests for portability within one month.

14.10. Where the request is complex, or a number of requests have been received, the timeframe can be extended by two months, ensuring that the individual is informed of the extension and the reasoning behind it within one month of the receipt of the request.

14.11. Where no action is being taken in response to a request, the Academy will, without delay and at the latest within one month, explain to the individual the reason for this and will inform them of their right to complain to the supervisory authority and to a judicial remedy.

15. The right to object

15.1. The Academy will inform individuals of their right to object at the first point of communication, and this information will be outlined in the privacy notice and explicitly brought to the attention of the data subject, ensuring that it is presented clearly and separately from any other information.

15.2. Individuals have the right to object to the following:

- Processing based on legitimate interests or the performance of a task in the public interest
- Direct marketing
- Processing for purposes of scientific or historical research and statistics.

15.3. Where personal data is processed for the performance of a legal task or legitimate interests:

- An individual's grounds for objecting must relate to his or her particular situation.

- The Academy will stop processing the individual's personal data unless the processing is for the establishment, exercise or defence of legal claims, or, where the Academy can demonstrate compelling legitimate grounds for the processing, which override the interests, rights and freedoms of the individual.

15.4. Where personal data is processed for direct marketing purposes:

- The Academy will stop processing personal data for direct marketing purposes as soon as an objection is received.
- The Academy cannot refuse an individual's objection regarding data that is being processed for direct marketing purposes.

15.5. Where personal data is processed for research purposes:

- The individual must have grounds relating to their particular situation in order to exercise their right to object.
- Where the processing of personal data is necessary for the performance of a public interest task, the Academy is not required to comply with an objection to the processing of the data.

15.6. Where the processing activity is outlined above, but is carried out online, the Academy will offer a method for individuals to object online.

16. Automated decision making and profiling

16.1. Individuals have the right not to be subject to a decision when:

- It is based on automated processing, e.g. profiling.
- It produces a legal effect or a similarly significant effect on the individual.

16.2. The Academy will take steps to ensure that individuals are able to obtain human intervention, express their point of view, and obtain an explanation of the decision and challenge it.

16.3. When automatically processing personal data for profiling purposes, the Academy will ensure that the appropriate safeguards are in place, including:

- Ensuring processing is fair and transparent by providing meaningful information about the logic involved, as well as the significance and the predicted impact.
- Using appropriate mathematical or statistical procedures.
- Implementing appropriate technical and organisational measures to enable inaccuracies to be corrected and minimise the risk of errors.
- Securing personal data in a way that is proportionate to the risk to the interests and rights of the individual and prevents discriminatory effects.

16.4. Automated decisions must not concern a child or be based on the processing of sensitive data, unless:

- The Academy has the explicit consent of the individual.
- The processing is necessary for reasons of substantial public interest on the basis of Union/Member State law.

17. Privacy by design and privacy impact assessments

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

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

17.3. DPIAs will allow the Academy to identify and resolve problems at an early stage, thus reducing associated costs and preventing damage from being caused to the Academy's reputation which might otherwise occur.

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

17.5. A DPIA will be used for more than one project, where necessary.

17.6. High risk processing includes, but is not limited to, the following:

- Systematic and extensive processing activities, such as profiling
- Large scale processing of special categories of data or personal data which is in relation to criminal convictions or offences
- The use of CCTV.

17.7. The Academy will ensure that all DPIAs include the following information:

- A description of the processing operations and the purposes
- An assessment of the necessity and proportionality of the processing in relation to the purpose
- An outline of the risks to individuals
- The measures implemented in order to address risk

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

18. Data breaches

18.1. 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.

18.2. The **Headteacher** will ensure that all staff members are made aware of, and understand, what constitutes a data breach as part of their CPD training.

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

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

18.5. 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.

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

18.7. A 'high risk' breach means that the threshold for notifying the individual is higher than that for notifying the relevant supervisory authority.

18.8. In the event that a breach is sufficiently serious, the public will be notified without undue delay.

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

18.10. Within a breach notification, the following information will be outlined:

- The nature of the personal data breach, including the categories and approximate number of individuals and records concerned
- The name and contact details of the DPO
- An explanation of the likely consequences of the personal data breach
- A description of the proposed measures to be taken to deal with the personal data breach
- Where appropriate, a description of the measures taken to mitigate any possible adverse effects

18.11. Failure to report a breach when required to do so may result in a fine, as well as a fine for the breach itself.

19. Data security

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

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

19.3. 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.

19.4. 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.

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

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

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

19.8. Staff, directors and Academy councillors will not use their personal laptops or computers for Academy purposes.

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

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

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

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

19.13. 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 Academy premises accepts full responsibility for the security of the data.

19.14. 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.

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

19.16. The physical security of the Academy'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.

19.17. The Trust takes its duties under the GDPR seriously and any unauthorised disclosure may result in disciplinary action.

19.18. The Trust is responsible for ensuring continuity and recovery measures are in place to ensure the security of protected data.

20. Publication of information

20.1. Classes of information that will be made routinely available include:

- Policies and procedures
- Minutes of meetings
- Annual reports
- Financial information

20.2. Classes of information specified above are made available quickly and easily on request.

20.3. Neither the Trust nor the Academy will publish any personal information, including photos, on their websites without the permission of the affected individual.

20.4. When uploading information to the Academy website, staff are considerate of any metadata or deletions which could be accessed in documents and images on the site.

21. CCTV and photography

21.1. The Academy understands that recording images of identifiable individuals constitutes as processing personal information, so it is done in line with data protection principles and the CCTV and surveillance policy.

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

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

21.4. All CCTV footage will be kept for a reasonable period of time for security purposes; the SBM is responsible for keeping the records secure and allowing access.

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

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

21.7. Precautions are taken when publishing photographs of pupils, in print, video or on the Academy website.

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

22. Data retention

22.1. Data will not be kept for longer than is necessary.

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

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

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

23. DBS data

23.1. All data provided by the DBS will be handled in line with data protection legislation; this includes electronic communication.

23.2. Data provided by the DBS will never be duplicated.

23.3. Any third parties who access DBS information will be made aware of the data protection legislation, as well as their responsibilities as a data handler.

1.2. CCTV and Monitoring Policy

1. Legal framework

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

- The Data Protection Act 2018
- The Regulation of Investigatory Powers Act 2000
- The Protection of Freedoms Act 2012
- The General Data Protection Regulation
- The Freedom of Information Act 2000
- The Education (Pupil Information) (England) Regulations 2005 (as amended in 2016)
- The Freedom of Information and Data Protection (Appropriate Limit and Fees) Regulations 2004
- The School Standards and Framework Act 1998
- The Children Act 1989
- The Children Act 2004
- The Equality Act 2010

1.2. This policy has been created with regard to the following statutory and non-statutory guidance:

- Home Office (2013) 'The Surveillance Camera Code of Practice'
- ICO (2017) 'Overview of the General Data Protection Regulation (GDPR)'
- ICO (2017) 'Preparing for the General Data Protection Regulation (GDPR) 12 steps to take now'
- ICO (2017) 'In the picture: A data protection code of practice for surveillance cameras and personal information'

1.3. This policy operates in conjunction with the GDPR Data Protection Policy.

1.4. The Data Protection Act 2018 and GDPR do not prevent the sharing of information for the purposes of keeping children safe in education. Fears about sharing information must not be allowed to stand in the way of the need to promote the welfare and protect the safety of children.

2. Definitions

For the purpose of this policy a set of definitions will be outlined, in accordance with the surveillance code of conduct:

Surveillance – monitoring the movements and behaviour of individuals; this can include video, audio or live footage. For the purpose of this policy only video and audio footage will be applicable.

Overt surveillance – any use of surveillance for which authority does not fall under the Regulation of Investigatory Powers Act 2000.

Covert surveillance – any use of surveillance which is intentionally not shared with the subjects it is recording. Subjects will not be informed of such surveillance.

The Trust does not normally use covert surveillance for the monitoring the Academy staff, pupils and/or volunteers. Covert surveillance will only be operable in exceptional circumstances and in compliance with the Data Protection Policy and in accordance with the Data Protection Act 2018.

Any overt surveillance footage will be clearly signposted around the Academy.

3. Roles and responsibilities

The role of the data protection officer (DPO) includes:

Dealing with freedom of information requests and subject access requests (SAR) in line with legislation, including the Freedom of Information Act 2000.

Ensuring that all data controllers at the Academy handle and process surveillance and CCTV footage in accordance with data protection legislation.

Ensuring that surveillance and CCTV footage is obtained in line with legal requirements.

Ensuring consent is clear, positive and unambiguous. Pre-ticked boxes and answers inferred from silence are non-compliant with the GDPR.

Ensuring that surveillance and CCTV footage is destroyed in line with legal requirements when it falls outside of its retention period.

Keeping comprehensive and accurate records of all data processing activities, including surveillance and CCTV footage, detailing the purpose of the activity and making these records public upon request.

Informing data subjects of how their data captured in surveillance and CCTV footage will be used by the Academy, their rights for the data to be destroyed and the measures implemented by the Academy to protect individuals' personal information.

Preparing reports and management information on the Academy's level of risk related to data protection and processing performance.

Reporting to the highest management level of the Academy, e.g. the governing board.

Abiding by confidentiality requirements in relation to the duties undertaken while in the role.

Monitoring the performance of the Academy's data protection impact assessment (DPIA) and providing advice where requested.

Presenting reports regarding data processing at the Academy to senior leaders and the governing board.

The Trust, as the corporate body, is the data controller. The Trust therefore has overall responsibility for ensuring that records are maintained, including security and access arrangements in accordance with regulations.

The Data Protection Officer deals with the day-to-day matters relating to data protection and thus, for the benefit of this policy will act as the data controller.

The role of the data controller includes:

Processing surveillance and CCTV footage legally and fairly.

Collecting surveillance and CCTV footage for legitimate reasons and ensuring that it is used accordingly.

Collecting surveillance and CCTV footage that is relevant, adequate and not excessive in relation to the reason for its collection.

Ensuring that any surveillance and CCTV footage identifying an individual is not kept for longer than is necessary.

Protecting footage containing personal data against accidental, unlawful destruction, alteration and disclosure – especially when processing over networks.

The role of the headteacher includes:

Liaising with the DPO to decide where CCTV is needed to justify its means.

Conferring with the DPO with regard to the lawful processing of the surveillance and CCTV footage.

Reviewing this Policy to ensure it is compliant with current legislation.

Monitoring legislation to ensure the Academy is using surveillance fairly and lawfully.

Communicating any changes to legislation with all members of staff.

4. Purpose and justification

The Trust will only use surveillance cameras for the safety and security of the academies within the Trust and its staff, pupils and visitors.

Surveillance will be used to protect health and safety and as a deterrent for violent behaviour and damage to the Academy or its staff or pupils.

The Academy will only conduct surveillance as a deterrent. Under no circumstances will the surveillance and the CCTV cameras be present in school classrooms, toilets or any changing facility.

If the surveillance and CCTV systems fulfil their purpose and are no longer required the Academy will deactivate them.

5. The data protection principles

Data collected from surveillance and CCTV 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 will 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.

6. Objectives

The surveillance system will be used to:

Maintain a safe environment.

Ensure the welfare of pupils, staff and visitors.

Deter criminal acts against persons and property.

Assist the police in identifying persons who have committed an offence.

7. Protocols

The surveillance system will be registered with the ICO in line with data protection legislation.

The surveillance system is a closed digital system which does not record audio.

Warning signs have been placed throughout the premises where the surveillance system is active, as mandated by the ICO's Code of Practice.

The surveillance system has been designed for maximum effectiveness and efficiency; however, the Academy cannot guarantee that every incident will be detected or covered and 'blind spots' may exist.

The surveillance system will not be trained on individuals unless an immediate response to an incident is required.

The surveillance system will not be trained on private vehicles or property outside the perimeter of the Academy.

8. Security

Access to the surveillance system, software and data will be strictly limited to authorised operators and will be password protected.

The Academy's authorised CCTV system operators are available upon request.

The main control facility is kept secure and locked when not in use.

If, in exceptional circumstances, covert surveillance is planned, or has taken place, copies of the Home Office's authorisation forms will be completed and retained.

Surveillance and CCTV systems will be tested for security flaws once a term to ensure that they are being properly maintained at all times.

Surveillance and CCTV systems will not be intrusive.

The DPO and headteacher will decide when to record footage, e.g. a continuous loop outside the academy grounds to deter intruders.

Any unnecessary footage captured will be retained no long than is reasonably necessary.

9. Privacy by design

The use of surveillance cameras and CCTV will be critically analysed using a DPIA, in consultation with the DPO.

A DPIA will be carried out prior to the installation of any surveillance and CCTV system.

If the DPIA reveals any potential security risks or other data protection issues, the Academy will ensure they have provisions in place to overcome these issues.

Where the Academy identifies a high risk to an individual's interests, and it cannot be overcome, the Academy will consult the ICO before they use CCTV, and the Academy will act on the ICO's advice.

The Academy will ensure that the installation of the surveillance and CCTV systems will always justify its means.

If the use of a surveillance and CCTV system is too privacy intrusive, the Academy will seek alternative provision.

10. Code of practice

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

The Academy notifies all pupils, staff and visitors of the purpose for collecting surveillance data via notice boards, letters and emails.

CCTV cameras are placed where they do not unreasonably intrude on anyone's privacy and are necessary to fulfil their purpose.

Surveillance footage will be kept no longer than is reasonably necessary; the headteacher and the data controller are responsible for keeping the records secure and allowing access.

The Academy has a surveillance system for the purpose of the prevention and detection of crime and the promotion of the health, safety and welfare of staff, pupils and visitors.

The surveillance and CCTV system is owned by the Academy and images from the system are strictly controlled and monitored by authorised personnel only.

The Academy will ensure that the surveillance and CCTV system is used to create a safer environment for staff, pupils and visitors to the Academy, and to ensure that its operation is consistent with the obligations outlined in data protection legislation. The policy is available from the Academy's website.

The surveillance and CCTV system will:

Be designed to take into account its effect on individuals and their privacy and personal data.

Be transparent and include a contact point, the DPO, through which people can access information and submit complaints.

Have clear responsibility and accountability procedures for images and information collected, held and used.

Have defined policies and procedures in place which are communicated throughout the Academy.

Only keep images and information for as long as reasonably required.

Restrict access to retained images and information with clear rules on who can gain access.

Consider all operational, technical and competency standards, relevant to the surveillance and CCTV system and its purpose, and work to meet and maintain those standards in accordance with the law.

Be subject to stringent security measures to safeguard against unauthorised access.

Be regularly reviewed and audited to ensure that policies and standards are maintained.

Only be used for the purposes for which it is intended, including supporting public safety, the protection of pupils, staff and volunteers, and law enforcement.

Be accurate and well maintained to ensure information is up-to-date.

11. Access

Under the GDPR, individuals have the right to obtain confirmation that their personal information is being processed.

All disks or storage containing images belong to, and remain the property of, the Tust.

Individuals have the right to submit an SAR to gain access to their personal data in order to verify the lawfulness of the processing.

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

A copy of the information will be supplied to the individual free of charge; however, the Academy may impose a 'reasonable fee' to comply with requests for further copies of the same information.

Where an SAR has been made electronically, the information will be provided in a commonly used electronic format.

Requests by persons outside the Academy for viewing or copying disks, or obtaining digital recordings, will be assessed by the headteacher, who will consult the DPO, on a case-by-case basis with close regard to data protection and freedom of information legislation.

Where a request is manifestly unfounded, excessive or repetitive, a reasonable fee will be charged.

All fees will be based on the administrative cost of providing the information.

All requests will be responded to without delay and usually within one month of receipt.

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.

Where a request is manifestly unfounded or excessive, the Academy holds the right to refuse to respond to the request. The individual will be informed of this decision and the reasoning behind it, as well as their right to complain to the ICO and to a judicial remedy, within one month of the refusal.

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

It is important that access to, and disclosure of, the images recorded by surveillance and CCTV footage is restricted and carefully controlled, not only to ensure that the rights of individuals are preserved, but also to ensure that the chain of evidence remains intact, should the images be required for evidential purposes.

Releasing the recorded images to third parties will be permitted only in the following limited and prescribed circumstances, and to the extent required or permitted by law:

The police – where the images recorded would assist in a specific criminal inquiry

Prosecution agencies – such as the Crown Prosecution Service (CPS)

Relevant legal representatives – such as lawyers and barristers

Persons who have been recorded and whose images have been retained where disclosure is required by virtue of data protection legislation and the Freedom of Information Act 2000

Requests for access or disclosure will be recorded and the headteacher will make the final decision as to whether recorded images may be released to persons other than the police.

12. Monitoring and review

This policy will be monitored and reviewed on an annual basis by the DPO and the Trust.

1.3. Biometric Data Policy

1. This policy

The Trust is committed to protecting the personal data of all its pupils and staff, this includes any biometric data we collect and process.

The Trust may collect and process biometric data in accordance with relevant legislation and guidance to ensure the data and the rights of individuals are protected.

This policy outlines the procedures the trust follows when collecting and processing biometric data.

This policy does not form part of any employee's contract of employment.

The Trust has overall responsibility for this policy, including keeping it under review.

This policy has due regard to all relevant legislation and guidance including, but not limited to the Protection of Freedoms Act 2012; Data Protection Act 2018; General Data Protection Regulation (GDPR); DfE (2018) *'Protection of biometric information of children in academy's and colleges'* and the Trust's Data Protection Policy.

2. Definitions

The following definitions apply in this policy:

"Biometric data": Personal information about an individual's physical or behavioural characteristics that can be used to identify that person, including their fingerprints, facial shape, retina and iris patterns, and hand measurements.

"Automated biometric recognition system": A system which measures an individual's physical or behavioural characteristics by using equipment that operates 'automatically' (i.e. electronically). Information from the individual is automatically compared with biometric information stored in the system to see if there is a match in order to recognise or identify the individual.

"Processing biometric data": Processing biometric data includes obtaining, recording or holding the data or carrying out any operation on the data including disclosing it, deleting it, organising it or altering it. An automated biometric recognition system processes data when:

Recording pupils/staff biometric data, e.g. taking measurements from a fingerprint via a fingerprint scanner.

Storing pupils/staff biometric information on a database.

Using pupils/staff biometric data as part of an electronic process, e.g. by comparing it with biometric information stored on a database to identify or recognise pupils.

"Special category data": Personal data which the GDPR says is more sensitive, and so needs more protection – where biometric data is used for identification purposes, it is considered special category data.

The Trust processes all personal data, including biometric data, in accordance with the key principles set out in the GDPR.

3. General Principles

The Trust will ensure biometric data is:

Processed lawfully, fairly and in a transparent manner.

Only collected for specified, explicit and legitimate purposes, and not further processed in a manner that is incompatible with those 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, and that reasonable steps are taken to ensure inaccurate information is rectified or erased.

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.

Processed in a manner that ensures appropriate security of the information, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.

4. Data Protection Impact Assessment

Prior to processing biometric data or implementing a system that involves processing biometric data, a Data Protection Impact Assessment (DPIA) will be carried out, which will:

Describe the nature, scope, context and purposes of the processing.

Assess necessity, proportionality and compliance measures.

Identify and assess risks to individuals.

Identify any additional measures to mitigate those risks.

When assessing levels of risk, the likelihood and the severity of any impact on individuals will be considered.

If a high risk is identified that cannot be mitigated, the DPO will consult the Information Commissioner's Officer (ICO) before the processing of the biometric data begins. The Trust will adhere to any advice from the ICO.

5. Consent

Please note that the obligation to obtain consent for the processing of biometric information of individuals under the age of 18 is not imposed by the Data Protection Act 2018 or the GDPR. Instead, the consent requirements for biometric information is imposed by section 26 of the Protection of Freedoms Act 2012.

Where the Trust uses pupil and staff biometric data as part of an automated biometric recognition system (e.g. using pupils' fingerprints to receive school lunch meals instead of paying with cash), the Trust will comply with the requirements of the Protection of Freedoms Act 2012.

In respect of pupils, written consent will be sought from at least one parent with parental responsibility for the pupil before the Trust collects or uses a pupil's biometric data.

The Trust will not process the biometric data of an individual under the age of 18 in the following circumstances:

They (verbally or non-verbally) object or refuse to participate in the processing of their biometric data;

No parent or carer has consented in writing to the processing;

A parent has objected in writing to such processing, even if another parent has given written consent.

Individuals (or their parents if under 18) can object to participation in the Trust's biometric system(s) or withdraw their consent at any time. Where this happens, any biometric data relating to the pupil that has already been captured will be deleted.

Where a pupil objects or refuses to participate, or to continue to participate, in activities that involve the processing of their biometric data, the trust will ensure that the pupil's biometric data is not taken or used as part of a biometric recognition system, irrespective of any consent given by the pupil's parent(s).

Where staff members or other adults use the trust's biometric system(s), consent will be obtained from them before they use the system. Staff and other adults can object to taking part in the trust's biometric system(s) and can withdraw their consent at any time. Where this happens, any biometric data relating to the individual that has already been captured will be deleted.

Where an individual object to taking part in the trust's biometric system(s), reasonable alternative arrangements will be provided that allow the individual to access the relevant service, e.g. where a biometric system uses pupil's fingerprints to pay for Academy meals, the pupil will be able to use cash for the transaction instead. Alternative arrangements will not put the individual at any disadvantage or create

difficulty in accessing the relevant service or result in any additional burden being placed on the individual (and the pupil's parents, where relevant).

6. Further information

Department for Education's 'Protection of Biometric Information of Children in Schools – https://www.gov.uk/government/publications/protection-of-biometric-information-ofchildren-in-schools

ICO guidance on data protection for education establishments - https://ico.org.uk/for-organisations/in-your-sector/education/