DATA PROTECTION POLICY

Policy Author	Principal Business Manager/CFO
Version	2
Date Last Reviewed	September 2021
Trust Key Reader	PE
Approved by Trust Board	March 2022
Review Date	September 2023
Circulation/Target Groups for this document	Trust Website, All Staff, Governors & Trustees

1. Introduction

1.1 This Policy sets out the obligations of Learner Engagement and Achievement Partnership Multi-Academy Trust (the Trust) regarding data protection and the rights of, inter alia, pupils, parents, staff and visitors ("data subjects") in respect of their personal data under the Data Protection Act 2018 and the associated UK GDPR including any subsequent amendments.

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

1.3 This Policy sets out the Trust's obligations regarding the collection, processing, transfer, storage, and disposal of personal data. The procedures and principles set out herein must be followed at all times by the Trust, its employees, agents, contractors, or other parties working on behalf of the Trust.

1.4 The Trust is committed not only to the letter of the law, but also to the spirit of the law and places high importance on the correct, lawful, and fair handling of all personal data, respecting the legal rights, privacy, and trust of all individuals with whom it deals.

2. The Data Protection Principles

2.1 This Policy aims to ensure compliance with the UK GDPR. The UK GDPR sets out the following principles with which any party handling personal data must comply. All personal data must be:

2.1.1 Processed lawfully, fairly, and in a transparent manner in relation to the data subject.

2.1.2 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.

2.1.3 Adequate, relevant, and limited to what is necessary in relation to the purposes for which it is processed.

2.1.4 Accurate and, where necessary, kept up to date. Every reasonable step must be taken to ensure that personal data that is inaccurate, having regard to the purposes for which it is processed, is erased, or rectified without delay.

2.1.5 Kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data is 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 UK GDPR in order to safeguard the rights and freedoms of the data subject.

2.1.6 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. The Rights of Data Subjects

3.1 The Data Protection Act 2018 and the UK GDPR sets out the following rights applicable to data subjects (please refer to the parts of this policy indicated for further details):

3.1.1 The right to be informed (Part 12).

3.1.2 The right of access (Part 13);

3.1.3 The right to rectification (Part 14);

3.1.4 The right to erasure (also known as the 'right to be forgotten') (Part 15);

3.1.5 The right to restrict processing (Part 16);

3.1.6 The right to data portability (Part 17);

3.1.7 The right to object (Part 18); and

3.1.8 Rights with respect to automated decision-making and profiling (Parts 19 and 20).

4. Lawful, Fair, and Transparent Data Processing

4.1 The UK GDPR seeks to ensure that personal data is processed lawfully, fairly, and transparently, without adversely affecting the rights of the data subject. The UK GDPR states that processing of personal data shall be lawful if at least one of the following applies:

4.1.1 The data subject has given consent to the processing of their personal data for one or more specific purposes

4.1.2 The processing is necessary for the performance of a contract to which the data subject is a party, or in order to take steps at the request of the data subject prior to entering into a contract with them

4.1.3 The processing is necessary for compliance with a legal obligation to which the data controller is subject

4.1.4 The processing is necessary to protect the vital interests of the data subject or of another natural person

4.1.5 The processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the data controller; or

4.1.6 The processing is necessary for the purposes of the legitimate interests pursued by the data controller or by a third party, except where such interests are overridden by the fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child.

4.2 If the personal data in question is "special category data" (also known as "sensitive personal data") (for example, data concerning the data subject's race, ethnicity, politics, religion, trade union membership, genetics, biometrics (if used for ID purposes), health, sex life, or sexual orientation), at least one of the following conditions must be met:

4.2.1 The data subject has given their explicit consent to the processing of such data for one or more specified purposes (unless UK law prohibits them from doing so)

4.2.2 The processing is necessary for the purpose of carrying out the obligations and exercising specific rights of the data controller or of the data subject in the field of employment, social security, and social protection law (insofar as it is authorised by UK law which provides for appropriate safeguards for the fundamental rights and interests of the data subject)

4.2.3 The processing is necessary to protect the vital interests of the data subject or of another natural person where the data subject is physically or legally incapable of giving consent

4.2.4 The data controller is a foundation, association, or other non-profit body with a political, philosophical, religious, or trade union aim, and the processing is carried out in the course of its legitimate activities, provided that the processing relates solely to the members or former members of that body or to persons who have regular contact with it in connection with its purposes and that the personal data is not disclosed outside the body without the consent of the data subjects

4.2.5 The processing relates to personal data which is clearly made public by the data subject

4.2.6 The processing is necessary for the conduct of legal claims or whenever courts are acting in their judicial capacity

4.2.7 The processing is necessary for substantial public interest reasons, on the basis of UK law which shall be proportionate to the aim pursued, shall respect the essence of the right to data protection, and shall provide for suitable and specific measures to safeguard the fundamental rights and interests of the data subject

4.2.8 The processing is necessary for the purposes of preventative or occupational medicine, for the assessment of the working capacity of an employee, for medical diagnosis, for the provision of health or social care or treatment, or the management of health or social care systems or services on the basis of UK law or pursuant to a contract with a health professional, subject to the conditions and safeguards referred to in Article 9(3) of the UK GDPR

4.2.9 The processing is necessary for public interest reasons in the area of public health, for example, protecting against serious cross-border threats to health or ensuring high standards of quality and safety of health care and of medicinal products or medical devices, on the basis of UK law which provides for suitable and specific measures to safeguard the rights and freedoms of the data subject (in particular, professional secrecy); or

4.2.10 The processing is necessary for archiving purposes in the public interest, scientific or historical research purposes, or statistical purposes in accordance with Article 89(1) of the UK GDPR based on UK law which shall be proportionate to the aim pursued, respect the essence of the right to data protection, and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject.

5. Specified, Explicit, and Legitimate Purposes

5.1 The Trust collects and processes the personal data set out in Part 21 of this Policy. This includes:

5.1.1 Personal data collected directly from data subjects; and

5.1.2 Personal data obtained from third parties

5.2 The Trust only collects, processes, and holds personal data for the specific purposes set out in Part 21 of this Policy (or for other purposes expressly permitted by the UK GDPR).

5.3 Data subjects are kept informed at all times of the purpose or purposes for which the Trust uses their personal data. Please refer to Part 12 for more information on keeping data subjects informed.

6. Adequate, Relevant, and Limited Data Processing

6.1 The Trust will only collect and process personal data for and to the extent necessary for the specific purpose or purposes of which data subjects have been informed (or will be informed) as under Part 5, above, and as set out in Part 21, below.

7. Accuracy of Data and Keeping Data Up-to-Date

7.1 The Trust shall ensure that all personal data collected, processed, and held by it is kept accurate and up-to-date. This includes, but is not limited to, the rectification of personal data at the request of a data subject, as set out in Part 14 below.

7.2 The accuracy of personal data shall be checked when it is collected and at regular intervals thereafter. If any personal data is found to be inaccurate or out-of-date, all reasonable steps will be taken without delay to amend or erase that data, as appropriate.

8. Data Retention

8.1 The Trust shall not keep personal data for any longer than is necessary in light of the purpose or purposes for which that personal data was originally collected, held, and processed

8.2 When personal data is no longer required, all reasonable steps will be taken to erase or otherwise dispose of it without delay

8.3 For full details of the Trust's approach to data retention, including retention periods for specific personal data types held by LEAP MAT, please refer to LEAP GDPR Records Management Policy.

9. Secure Processing

9.1 The Trust shall ensure that all personal data collected, held, and processed is kept secure and protected against unauthorised or unlawful processing and against accidental loss, destruction, or damage. Further details of the technical and organisational measures which shall be taken are provided in Parts 22 to 27 of this Policy.

10. Accountability and Record-Keeping

10.1 The Trust's Data Protection Officer's details and Information Commissioners Office (ICO) registration number are provided at the end of this policy.

10.2 The Data Protection Officer shall be responsible for overseeing the implementation of this Policy and for monitoring compliance with this Policy, the Trust's other data protection-related policies, and with the UK GDPR and other applicable data protection legislation.

10.3 The Trust shall keep written internal records of all personal data collection, holding, and processing, which shall incorporate the following information:

10.3.1 The name and details of the Trust, its Data Protection Officer, and any applicable third-party data processors

10.3.2 The purposes for which The Trust collects, holds, and processes personal data

10.3.3 Details of the categories of personal data collected, held, and processed by The Trust, and the categories of data subject to which that personal data relates

10.3.4 Details of any transfers of personal data to countries without a suitable adequacy decision from the UK Government, including all mechanisms and security safeguards

10.3.5 Details of how long personal data will be retained by the Trust (please refer to our *LEAP GDPR Records Management Policy*); and

10.3.6 Detailed descriptions of all technical and organisational measures taken by the Trust to ensure the security of personal data.

11. Data Protection Impact Assessments

11.1 The Trust shall carry out Data Protection Impact Assessments for any and all new projects and/or new uses of personal data which involve the use of new technologies and the processing involved is likely to result in a high risk to the rights and freedoms of data subjects under the UK GDPR.

11.2 Data Protection Impact Assessments shall be overseen by the Data Protection Officer, supported by the Academy GDPR Leads. DPIAs shall address the following:

11.2.1 The type(s) of personal data that will be collected, held, and processed
11.2.2 The purpose(s) for which personal data is to be used
11.2.3 The Trust's objectives
11.2.4 How personal data is to be used
11.2.5 The parties (internal and/or external) who are to be consulted
11.2.6 The necessity and proportionality of the data processing with respect to the purpose(s) for which it is being processed
11.2.7 Risks posed to data subjects
11.2.8 Risks posed both within and to the Trust; and
11.2.9 Proposed measures to minimise and handle identified risks.

12. Keeping Data Subjects Informed

12.1 The Trust shall provide the information set out in Part 12.2 to every data subject:

12.1.1 Where personal data is collected directly from data subjects, those data subjects will be informed of its purpose at the time of collection; and

12.1.2 Where personal data is obtained from a third party, the relevant data subjects will be informed of its purpose:
a) if the personal data is used to communicate with the data subject, when the first communication is made; or
b) if the personal data is to be transferred to another party, before that transfer is made; or
c) as soon as reasonably possible and in any event not more than one month after the personal data is obtained.

12.2 The following information shall be provided:

12.2.1 Details of the Trust including, but not limited to, the identity of its Data Protection Officer

12.2.2 The purpose(s) for which the personal data is being collected and will be processed (as detailed in Part 21 of this Policy) and the legal basis justifying that collection and processing

12.2.3 Where applicable, the legitimate interests upon which the Trust is justifying its collection and processing of the personal data

12.2.4 Where the personal data is not obtained directly from the data subject, the categories of personal data collected and processed

12.2.5 Where the personal data is to be transferred to one or more third parties, details of those parties

12.2.6 Where the personal data is to be transferred to a third party that is located in a territory without an adequacy agreement as approved by the UK Government, details of that transfer, including but not limited to the safeguards in place (see Part 28 of this Policy for further details)

12.2.7 Details of data retention

12.2.8 Details of the data subject's rights under the UK GDPR

12.2.9 Details of the data subject's right to withdraw their consent to the Trust's processing of their personal data at any time

12.2.10 Details of the data subject's right to complain to the Information Commissioner's Office (the "supervisory authority" under the UK GDPR)

12.2.11 Where applicable, details of any legal or contractual requirement or obligation necessitating the collection and processing of the personal data and details of any consequences of failing to provide it; and

12.2.12 Details of any automated decision-making or profiling that will take place using the personal data, including information on how decisions will be made, the significance of those decisions, and any consequences.

13. Data Subject Access

13.1 Data subjects may make subject access requests ("SARs") at any time to find out more about the personal data which the Trust holds about them, what it is doing with that personal data, and why. They are encouraged to make these requests by emailing the relevant academy at GDPR-lead@bri.leap-mat.org.uk, GDPR-lead@din.leap-mat.org.uk, and GDPR-lead@eck.leap-mat.org.uk.

13.2 Employees wishing to make a SAR should contact the relevant GDPR lead: GDPR-lead@bri.leap-mat.org.uk, GDPR-lead@din.leap-mat.org.uk, or GDPR-lead@eck.leap-mat.org.uk.

13.3 Responses to SARs shall normally be made within one month of receipt, however this may be extended by up to two months if the SAR is complex and/or numerous requests are made. If such additional time is required, the data subject shall be informed.

13.4 Responses to SARs shall be dependent upon the terms of the UK GDPR, the Data Protection Act (2018) and associated ICO guidance.

13.5 The Trust does not charge a fee for the handling of normal SARs. The Trust reserves the right to charge reasonable fees for additional copies of information that has already been supplied to a data subject, and for requests that are manifestly unfounded or excessive, particularly where such requests are repetitive.

14. Rectification of Personal Data

14.1 Data subjects may have the right to require the Trust to rectify any of their personal data that is inaccurate or incomplete.

14.2 Where such rectification is possible, The Trust shall rectify the personal data in question, and inform the data subject of that rectification, within one month of the data subject informing the Trust of the issue. The period can be extended by up to two months in the case of complex requests. If such additional time is required, the data subject shall be informed.

14.3 In the event that any affected personal data has been disclosed to third parties, those parties shall be informed of any rectification that must be made to that personal data.

15. Erasure of Personal Data

15.1 Data subjects have the right to request that the Trust erases the personal data it holds about them in the following circumstances:

15.1.1 It is no longer necessary for The Trust to hold that personal data with respect to the purpose(s) for which it was originally collected or processed

15.1.2 The data subject wishes to withdraw their consent to the Trust holding and processing their personal data

15.1.3 The data subject objects to The Trust holding and processing their personal data (and there is no overriding legitimate interest to allow the Trust to continue doing so) (see Part 18 of this Policy for further details concerning the right to object)

15.1.4 The personal data has been processed unlawfully

15.1.5 The personal data needs to be erased in order for The Trust to comply with a particular legal obligation; or

15.1.6 The personal data is being held and processed for the purpose of providing information society services to a child.

15.2 Unless the Trust has reasonable grounds to refuse to erase personal data, all requests for erasure shall be complied with, and the data subject informed of the erasure, within one month of receipt of the data subject's request. The period can be extended by up to two months in the case of complex requests. If such additional time is required, the data subject shall be informed.

15.3 In the event that any personal data that is to be erased in response to a data subject's request has been disclosed to third parties, those parties shall be informed of the erasure (unless it is impossible or would require disproportionate effort to do so).

16. Restriction of Personal Data Processing

16.1 Data subjects may request that the Trust restricts processing the personal data it holds about them. If a data subject makes such a request, The Trust shall in so far as is possible ensure that the personal data is only stored and not processed in any other fashion.

16.2 If the Trust is required to process the data for statutory purposes or for reasons of legal compliance, then the Trust shall inform the Data Subject that this processing is expected to take place. If possible, this notice will be provided prior to processing.

16.3 In the event that any affected personal data has been disclosed to third parties, those parties shall be informed of the applicable restrictions on processing it (unless it is impossible or would require disproportionate effort to do so).

17. Data Portability

17.1 The Trust processes personal data using automated means. Such processing is carried out by, inter alia, our management information system (Integris), our human resources systems and our catering management system.

17.2 Where data subjects have given their consent to the Trust to process their personal data in such a manner, or the processing is otherwise required for the performance of a contract between the Trust and the data subject, data subjects have the right, under the UK GDPR, to receive a copy of their personal data and to use it for other purposes (namely transmitting it to other data controllers).

17.3 Where technically feasible, if requested by a data subject, personal data shall be sent directly to the required data controller.

17.4 All requests for copies of personal data shall be complied with within one month of the data subject's request. The period can be extended by up to two months in the case of complex or numerous requests. If such additional time is required, the data subject shall be informed.

18. Objections to Personal Data Processing

18.1 Data subjects have the right to object to the Trust processing their personal data based on performing a task in the public interest. Its' legitimate interests, or direct marketing (including profiling).

18.2 Where a data subject objects to the Trust processing their personal data, the Trust shall cease such processing immediately, unless it can be demonstrated that the Trust's grounds for such processing override the data subject's interests, rights, and freedoms, or that the processing is necessary for the conduct of legal claims.

18.3 Where a data subject objects to the Trust processing their personal data for direct marketing purposes, the Trust shall cease such processing immediately.

18.4 Where a data subject objects to the Trust processing their personal data for scientific and/or historical research and statistics purposes, the data subject must, under the UK GDPR, "demonstrate grounds relating to his or her particular situation". The Trust is not required to comply if the research is necessary for the performance of a task carried out for reasons of public interest.

19. Automated Decision-Making

19.1 The Trust is not currently using personal data in automated decision-making processes. In the event that that this situation changes, the Trust shall notify data subjects of its' intentions to commence such processing.

19.2 Where such decisions have a legal (or similarly significant effect) on data subjects, those data subjects have the right to challenge to such decisions under the UK GDPR, requesting human intervention, expressing their own point of view, and obtaining an explanation of the decision from the Trust.

19.3 The right described in Part 19.2 does not apply in the following circumstances:
- 19.3.1 The decision is necessary for the entry into, or performance of, a contract between the Trust and the data subject
- 19.3.2 The decision is authorised by law; or
- 19.3.3 The data subject has given their explicit consent.

20. Profiling

20.1 The Trust uses personal data for profiling purposes. These purposes relate to helping student maximise achievement and monitor staff performance.

20.2 When personal data is used for profiling purposes, the following shall apply:
- 20.2.1 Clear information explaining the profiling shall be provided to data subjects, including the significance and likely consequences of the profiling
- 20.2.2 Appropriate mathematical or statistical procedures shall be used
- 20.2.3 Technical and organisational measures shall be implemented to minimise the risk of errors. If errors occur, such measures must enable them to be easily corrected; and
- 20.2.4 All personal data processed for profiling purposes shall be secured in order to prevent discriminatory effects arising out of profiling (see Parts 22 to 26 of this Policy for more details on data security).

21. Personal Data Collected, Held and Processed

21.1 Individuals will be informed how the Trust processes its data through privacy notices and associated policies (available on each school's website). Internal records of processing activities will be maintained. This will include the Trust's legal basis for processing certain types of personal and sensitive data. Please see Section 8 of this policy regarding the Trust's Records Management, which outlines the records that the Trust will maintain.

21.2

22. Data Security - Transferring Personal Data and Communications

22.1 The Trust shall ensure that the appropriate measures are taken with respect to all communications and other transfers involving personal data:
- 22.1.1 Personal data may be transmitted over secure networks only; transmission over unsecured networks is not permitted in any circumstances
- 22.1.2 The Trust will ensure that where special category personal data or other sensitive information is sent in the post that it shall be possible to demonstrate that it was delivered.
- 22.1.3 Where special category personal data or other sensitive information is to be shared with a third-party it shall be sent by MS Office 365's OneDrive / SharePoint via a secure link to a verified email address using the "Can View". Where it has to be shared by a "*Can Edit*" link in O365 (i.e. downloadable), the document must be encrypted using 7Zip, and the password communicated to the intended recipient using a verified source.
- 22.1.4 Where personal data is to be transferred in removal storage devices, these devices shall be encrypted. The use of unencrypted removable storage devices is prohibited by The Trust unless specifically approved by the Chief Executive.

23. Data Security - Storage

23.1 The Trust shall ensure that the following measures are taken with respect to the storage of personal data:

23.1.1 All electronic copies of personal data should be stored securely using passwords, user access rights and where appropriate data encryption

23.1.2 The physical security of all Trust sites, buildings and storage systems, and access to them, must be maintained to an appropriate standard

23.1.3 All hardcopies of personal data, along with any electronic copies stored on physical, removable media should be stored securely in a locked box, drawer, cabinet, or similar

23.1.4 All personal data stored electronically, should be backed up according to IT Policies

23.1.5 Where any member of staff stores personal data on a Trust mobile device (a computer, tablet, phone or any other device) that member of staff must abide by the *Trust's Staff Acceptable Use Policy*. The member of staff shall also ensure that they can provide a secure environment for that device to be used so as to minimise any risk to the confidentiality or integrity of the information.

24. Data Security - Disposal

24.1 When any personal data is to be erased or otherwise disposed of for any reason (including where copies have been made and are no longer needed), it should be securely deleted and disposed of. For further information on the deletion and disposal of personal data, please refer to the Trust's *LEAP GDPR Records Management Policy*.

25. Data Security - Use of Personal Data

25.1 The Trust shall ensure that the following measures are taken with respect to the use of personal data:

25.1.1 No personal data may be shared informally and if an employee, agent, sub-contractor, or other party working on behalf of The Trust requires access to any personal data that they do not already have access to, such access should be formally requested from the GDPR Lead.

25.1.2 No personal data may be transferred to any employees, agents, contractors, or other parties, whether such parties are working on behalf of The Trust or not, without authority

25.1.3 Personal data must be handled with care at all times and should not be left unattended or on view to unauthorised employees, agents, sub-contractors, or other parties at any time

25.1.4 If personal data is being viewed on a computer screen and the computer in question is to be left unattended, the user must lock the computer and screen before leaving it (on MS Windows Machines - WindowsKey & 'L' Key or via the Alt-Ctrl-Del menu)

25.1.5 Where it is considered necessary for personal data to be taken off LEAP premises, either in electronic or paper format, staff will take extra care to follow the same procedures for security, e.g. use of lock and key. The person taking the information from LEAP premises accepts full responsibility for the security of the personal data. The personal data must remain with the member of staff at all times during transit, which should be taken directly to the destination premises. The data must not be left in an unattended vehicle. Unless in the direct personal possession or the data is being accessed by the member of staff, the data must be in a locked box, drawer, cabinet,

or similar under the member of staff's control. The data must be directly returned by the member of staff to LEAP premises and securely stored; and

25.1.6 Where personal data held by the Trust is used for marketing purposes, it shall be the responsibility of the member of LEAP staff intending to use to ensure that the appropriate consent is obtained and that no data subjects have opted out, whether directly or via a third-party service.

26. Data Security - IT Security

26.1 Full details of the Trust's IT security requirements and procedures can be found in LEAP's ICT Infrastructure Security Breach Prevention and Management Plan and the LEAP's Staff Acceptable Use Policy. The Trust shall ensure that, the following matters are addressed with respect to IT and information security:

- Assignment of responsibilities for identified key personnel
- Access authentication requirements, recognising the need for dual authentication, as necessary, and password requirements, including complexity
- User Privileges
- Secure System Configuration, including installation of software which processes personal data
- Network Security
- Malware Prevention
- Monitoring Usage
- Removable Media and Home Working
- Backing-Up Data and Restoration of Systems and Data
- User Training and Awareness
- Security Breach Incidents

27. Biometric recognition systems

Where LEAP use pupils' biometric data,for example, measurements are taken from a pupil's finger prints to access their on line school food account, instead of paying with cash we will comply with the requirements of the Protection of Freedoms Act 2012.

Parents'/carers' written consent will be sought before collecting any biometric data.

Notification sent to parents will include information about the processing of their child's biometric information that is sufficient to ensure that parents are fully informed about what is being proposed. This will include: details about the type of biometric information to be taken; how it will be used; the parents' and the pupil's right to refuse or withdraw their consent; and details of alternative arrangements for those who refuse.

The school does not need to notify a particular parent or seek their consent if it is satisfied that:
• The parent cannot be found, e.g. their whereabouts or identity is not known.
• The parent lacks the mental capacity to object or consent.
• The welfare of the pupil requires that a particular parent is not contacted, e.g. where a pupil has been separated from an abusive parent who must not be informed of the pupil's whereabouts.
• It is otherwise not reasonably practicable for a particular parent to be notified or for their consent to be obtained.

Where neither of the parents of a child can be notified for one of the reasons set out above (which would mean consent cannot be obtained from either of them), the following must be considered:

• If the child is being 'looked after' by a local authority or is accommodated or maintained by a voluntary organisation (i.e. a not-for-profit organisation), the local authority, or as the case may be, the voluntary organisation must be notified and their written consent obtained.
• If the paragraph above does not apply, then notification must be sent to all those caring for the child and written consent must be gained from at least one carer before the child's biometric data can be processed (subject to the child and none of the carers objecting in writing).

LEAP will take reasonable steps to locate a parent before they are able to rely on the exemption (i.e. notification of a parent not required if the parent cannot be found).

Parents/carers and pupils can withdraw consent, at any time, and we will make sure that any relevant data already captured is deleted.

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

As required by law, if a pupil refuses to participate in, or continue to participate in, the processing of their biometric data, we will not process that data irrespective of any consent given by the pupil's parent(s)/carer(s).

Where staff members or other adults use the school's biometric system(s), we will also obtain their consent before they first take part in it, and provide alternative means of accessing the relevant service if they object. Staff and other adults can also withdraw consent at any time, and the school will delete any relevant data already captured.

28. Organisational Measures

28.1 The Trust shall ensure that the following measures are taken with respect to the collection, holding, and processing of personal data:

28.1.1 All employees, agents, contractors, or other parties working on behalf of The Trust shall be made fully aware of both their individual responsibilities and our responsibilities under the UK GDPR and under this Policy, and shall have free access to a copy of this Policy

28.1.2 Only employees, agents, sub-contractors, or other parties working on behalf of the Trust that need access to, and use of, personal data in order to carry out their assigned duties correctly shall have access to personal data held by the Trust

28.1.3 All employees, agents, contractors, or other parties working on behalf of the Trust handling personal data will be appropriately trained to do so

28.1.4 All employees, agents, contractors, or other parties working on behalf of the Trust handling personal data will be appropriately supervised

28.1.5 All employees, agents, contractors, or other parties working on behalf of the Trust handling personal data shall be required and encouraged to exercise care, caution, and discretion when discussing work-related matters that relate to personal data, whether in the workplace or otherwise

28.1.6 Methods of collecting, holding, and processing personal data shall be regularly evaluated and reviewed

28.1.7 All personal data held by the Trust shall be reviewed periodically, as set out in the *LEAP GDPR Records Management Policy*

28.1.8 The performance of those employees, agents, contractors, or other parties working on behalf of the Trust handling personal data shall be regularly evaluated and reviewed

28.1.9 The contravention of these rules will be treated as a disciplinary matter

28.1.10 All employees, agents, contractors, or other parties working on behalf of the Trust handling personal data will be bound to do so in accordance with the principles of the UK GDPR and this Policy by contract

28.1.11 All agents, contractors, or other parties working on behalf of the Trust handling personal data must ensure that any and all of their employees who are involved in the processing of personal data are held to the same conditions as those relevant employees of the Trust arising out of this Policy and the UK GDPR; and

28.1.12 Where any agent, contractor or other party working on behalf of the Trust handling personal data fails in their obligations under this Policy that party shall indemnify and hold harmless the Trust against any costs, liability, damages, loss, claims or proceedings which may arise out of that failure.

29. Transferring Personal Data to a Country Without an Adequacy Decision

29.1 The Trust may from time to time transfer ('transfer' includes making available remotely) personal data to countries without a suitable adequacy decision from the UK Government.

29.2 The transfer of personal data to a country without an adequacy decision shall take place only if one or more of the following applies:

28.2.1 The transfer is to a country, territory, or one or more specific sectors in that country (or an international organisation), that the UK Government has determined ensures an adequate level of protection for personal data

29.2.2 The transfer is to a country (or international organisation) which provides appropriate safeguards in the form of a legally binding agreement between public authorities or bodies; binding corporate rules; standard data protection clauses adopted by the UK Government compliance with an approved code of conduct approved by a supervisory authority (e.g. the Information Commissioner's Office); certification under an approved certification mechanism (as provided for in the UK GDPR); contractual clauses agreed and authorised by the competent supervisory authority; or provisions inserted into administrative arrangements between public authorities or bodies authorised by the competent supervisory authority

29.2.3 The transfer is made with the informed consent of the relevant data subject(s)

29.2.4 The transfer is necessary for the performance of a contract between the data subject and the Trust (or for pre-contractual steps taken at the request of the data subject)

29.2.5 The transfer is necessary for important public interest reasons

29.2.6 The transfer is necessary for the conduct of legal claims

29.2.7 The transfer is necessary to protect the vital interests of the data subject or other individuals where the data subject is physically or legally unable to give their consent; or

29.2.8 The transfer is made from a register that, under UK or EU law, is intended to provide information to the public and which is open for access by the public in general or otherwise to those who are able to show a legitimate interest in accessing the register.

30. Data Breach Notification

30.1 All personal data breaches must be reported immediately to the *GDPR Lead* in the relevant Academy who will inform the Data Protection Officer.

30.2 If a personal data breach occurs and that breach is likely to result in a risk to the rights and freedoms of data subjects (e.g. financial loss, breach of confidentiality, discrimination, reputational damage, or other significant social or economic damage), the Data Protection Officer must ensure that the Information Commissioner's Office is informed of the breach without delay, and in any event, within 72 hours after having become aware of it.

30.3 In the event that a personal data breach is likely to result in a high risk (that is, a higher risk than that described under Part 29.2) to the rights and freedoms of data subjects, the Data Protection Officer must ensure that all affected data subjects are informed of the breach directly and without undue delay.

30.4 Data breach notifications shall include the following information:

30.4.1 The categories and approximate number of data subjects concerned

30.4.2 The categories and approximate number of personal data records concerned

30.4.3 The name and contact details of the Trust's data protection officer (or other contact point where more information can be obtained)

30.4.4 The likely consequences of the breach

29.4.5 Details of the measures taken, or proposed to be taken, by the Trust to address the breach including, where appropriate, measures to mitigate its possible adverse effects.

31. Implementation of Policy

31.1 No part of this Policy shall have retroactive effect and shall thus apply only to matters occurring on or after its adoption.

32. Data Protection Officer & ICO Registration number

Name of Data Protection Officer: Mr R Wheatcroft
Email address: DPO@leap-mat.org.uk
LEAP Trust ICO Registration Number: Z2447291

GDPR Leads in each school

GDPR-lead@bri.leap-mat.org.uk
GDPR-lead@din.leap-mat.org.uk
GDPR-lead@eck.leap-mat.org.uk