Data Protection Policy

Approved	The Trust Board	**Date: October 2024**
Last reviewed:	Autumn 24	
Next review due by:	Autumn 25	

Contents

1. INTRODUCTION. 3
2. KEY DEFINITIONS 3
2.1. Personal Data 3
2.2. Data Subject 4
2.3. Data Controller 4
2.4. Data Processor 4
3. ORGANISATIONAL ARRANGEMENTS 4
3.1. Overall responsibility 4
3.2. Data Registration 5
3.3. Data Protection Officer 5
4. THE DATA PROTECTION PRINCIPLES 5
5. CONDITIONS FOR PROCESSING IN THE FIRST DATA PROTECTION PRINCIPLE 6
6. CONDITIONS FOR PROCESSING IN THE SECOND DATA PROTECTION PRINCIPLE 7
7. CONDITIONS FOR PROCESSING IN THE THIRD DATA PROTECTION PRINCIPLE 7
8. CONDITIONS FOR PROCESSING IN THE FOURTH DATA PROTECTION PRINCIPLE 7
9. CONDITIONS FOR PROCESSING IN THE FIFTH DATA PROTECTION PRINCIPLE 7
10. CONDITIONS FOR PROCESSING IN THE SIXTH DATA PROTECTION PRINCIPLE 7
11. CONDITIONS FOR PROCESSING IN THE SEVENTH DATA PROTECTION PRINCIPLE 8
12. USE OF PERSONAL DATA BY THE TRUST 8
12.2. Pupils 8
12.3. Staff 8
12.5. Other Individuals 9
13. DISCLOSURE OF PERSONAL DATA TO THIRD PARTIES 9
14. CONFIDENTIALITY OF PUPIL CONCERNS 10
15. DATA SUBJECT RIGHTS 10
16. The right to be informed 10
17. The right of access 11
18. The right to rectification 11
19. The right to erasure 11
20. The right to restrict processing 12
21. The right to data portability 12
22. The right to object. 13
23. Rights related to automated decision making and profiling. 13
24. BIOMETRIC RECOGNITION SYSTEMS. 14
25. CCTV 14
26. BREACH OF ANY REQUIREMENT OF THE GDPR 14
27. CONTACT 15
28. COMPLAINTS 15

1. INTRODUCTION.

1.1. The Unity Schools Partnership and the schools therein ("the Trust") collect and process certain types of personal data about staff, pupils, parents and other individuals who come into contact with the Trust in order to provide education and associated functions.

1.2. The Trust may be required by law to collect and use certain types of data to comply with statutory obligations related to employment, education, and safeguarding. This policy is intended to ensure that personal data is dealt with properly and securely and in accordance with the UK General Data Protection Regulation (UK GDPR) and other related legislation, including the Data Protection Act 2018 (DPA 2018).

1.3. This policy will be updated as necessary to reflect best practice, or amendments made to data protection legislation, and shall be reviewed annually.

1.4. This policy, and the processes herein apply to all manual files and computerised data, if they come within the definition of a filing system. Broadly speaking, a filing system is one where the data is structured in some way that it is searchable on the basis of specific criteria (for example, you would be able to use something like the individual's name to find their information), and if this is the case, it does not matter whether the information is located in a different physical location.

2. KEY DEFINITIONS

2.1. **Personal Data**

2.1.1. The DPA outlines how organisations, including Unity Schools Partnership, must collect, handle and store personal information ('personal data').

2.1.2. 'Personal data' is any information that identifies a living individual and includes information that would identify an individual to the person to whom it is disclosed because of any special knowledge that they have or can obtain[11].

2.1.3. Personal data can be stored within manual files or as computerised data.

2.1.4. A sub-set of personal data is known as 'special category personal data'. This special category data is:

- personal data revealing racial or ethnic origin;
- personal data revealing political opinions;
- personal data revealing religious or philosophical beliefs;
- personal data revealing trade union membership;
- genetic data;
- biometric data (where used for identification purposes);
- data concerning health;
- data concerning a person's sex life; and

[1] For example, if asked for the number of female employees, and you only have one female employee, this would be personal data if it was possible to obtain a list of employees from the website.

- data concerning a person's sexual orientation.

2.1.5. Special Category Data is given special protection, and additional safeguards apply if this information is to be collected and used.

2.1.6. The Trust does not intend to seek or hold Special Category Data (previously known as sensitive personal data) about staff or pupils except where the Trust has been notified of the information, or it comes to the Trust's attention via legitimate means (e.g. a grievance) or needs to be sought and held in compliance with a legal obligation or as a matter of good practice. Staff or pupils are under no obligation to disclose to the Trust their racial or ethnic origin, political or religious beliefs, whether or not they are a trade union member or details of their sexual life (save to the extent that details of marital status and / or parenthood are needed for other purposes, e.g. pension entitlements).

2.1.7. Information relating to criminal convictions shall only be held and processed where there is legal authority to do so.

2.2. Data Subject

2.2.1. A 'Data Subject' is someone whose details the Trust gather or process for any reason.

2.2.2. The data subject has rights under the UK GDPR, as defined in section 4 below.

2.2.3. In some cases, the obligations of the Trust to share data with other organisations, including but not limited to the Department for Education (DfE) and the Local Authority (LA) may override these rights under the UK GDPR.

2.3. Data Controller

2.3.1. For the purpose of this policy, Unity Schools Partnership is the 'Data Controller'

2.3.2. The 'Data Controller' has overall responsibility for the personal data gathered and processed, and has responsibility for ensuring compliance with the relevant legislation. The 'Data Controller' is able to delegate this to 'Data Processors' to act on their behalf.

2.4. Data Processor

2.4.1. For the purpose of this policy, the 'Data Processor' may be a member of staff, third party company or another organisation including but not limited to the DfE or Local Authority.

2.4.2. The 'Data Processor' is the person or organisation which uses, collects, accesses or amends the data that the 'Data Controller' is authorised to collect or has already collected.

3. ORGANISATIONAL ARRANGEMENTS

3.1. Overall responsibility

3.1.1. The Trust has an overall responsibility to put in place clear policies and procedures and to monitor these processed to ensure that measures have been implemented and remain appropriate and effective.

3.1.2. Each school within the Trust will ensure that they have designated staff who are appropriately trained to ensure data protection is managed appropriately, in accordance with this policy.

3.1.3. All staff are responsible for acting in accordance with the data protection principles and respecting an individual's rights under the GDPR, and should complete annual GDPR

training to support this.

3.2. Data Registration

3.2.1. As a Data Controller, the Trust must register as a Data Controller on the Data Protection Register as held by the Information Commissioner's Office. The Trust was last registered on 25th June 2023 and is due to renew on 25th June 2024.

3.3. Data Protection Officer

3.3.1. As a public body, the Trust is required to appoint a Data Protection Officer (DPO)

3.3.2. At Unity Schools Partnership, this role is fulfilled by Mr Michael Vaughan, who can be contacted via dpo@unitysp.co.uk

3.3.3. The role of the DPO is to:

- Inform and advise the Trust, it's schools and all employees about obligations to comply with all relevant data protection laws.
- Monitor compliance with the relevant data protection laws.
- Be the first point of contact for supervisory authorities.

4. THE DATA PROTECTION PRINCIPLES

4.1. The seven data protection principles as laid down in the GDPR are followed at all times:

- personal data shall be processed fairly, lawfully and in a transparent manner, and processing shall not be lawful unless one of the 6 processing conditions defined in Schedule 9 of the DPA can be met;
- personal data shall be collected for specific, explicit, and legitimate purposes, and shall not be further processed in a manner incompatible with those purposes;
- personal data shall be adequate, relevant, and limited to what is necessary for the purpose(s) for which it is being processed;
- personal data shall be accurate and, where necessary, kept up to date;
- personal data processed for any purpose(s) shall not be kept in a form which permits identification of individuals for longer than is necessary for that purpose / those purposes;
- personal data shall be processed in such a way that ensures appropriate security of the data, including protection against unauthorised or unlawful processing and against accidental loss, destruction, or damage, using appropriate technical or organisational measures.
- appropriate measures and records must be in place to be able to demonstrate compliance with the other principles.

4.2. The Trust is committed to complying with the principles in section 4 at all times, as set out in sections 4 – 11 below.

4.3. In addition to this, the trust is committed to:

4.3.1. ensuring that at all times, anyone dealing with personal data shall be mindful of the individual's rights under the law (as explained in more detail in).

4.3.2. ensuring that any breaches of the DPA are reported in accordance with the

procedure in section

4.3.3. ensuring that clear procedures are set out for responding to any personal data requests in accordance with the individual's rights under the GDPR.

5. CONDITIONS FOR PROCESSING IN THE FIRST DATA PROTECTION PRINCIPLE

5.1. In order to comply with the fair processing requirements of the DPA, The Trust will inform all staff, pupils, parents and carers, governors and trustees, and any other individuals, of the data they collect, process and hold on them, the purposes for which the data is held and the third parties (e.g. LA, DfE, etc) to whom their data may be passed, through the use of privacy notices which we issue via our website – more information about our privacy notices can be found in section 16 below.

5.2. To ensure lawfulness of processing, one of the following conditions must be met:

5.2.1.1. The individual has given consent that is specific to the particular type of processing activity.

5.2.1.2. Consent is defined by the DPA as "any freely given, specific, informed and unambiguous indication of the data subject's wishes by which they, by a statement or by clear affirmative action, signifies agreement to the processing of personal data relating to them".

5.2.1.3. The Trust will seek consent from staff, volunteers, young people, parents and carers to collect and process their data. We will be clear about our reasons for requesting the data and how we will use it.

5.2.1.4. Where the individual is under 12 years of age, or where the individual is 12 years or older but is understood to lack capacity to consent (for example, where there is evidence of special educational needs which effect the individual's mental capacity to understand their rights), a person with parental responsibility has given consent on their behalf, that is specific to the particular type of processing activity, and that consent is informed, unambiguous and freely given.

5.2.1.5. There may be contractual, statutory and regulatory occasions when consent is not required; in these circumstances, one of the other conditions for processing will apply.

5.2.1.6. For any processing is done on the basis of consent, consent can be withdrawn by the individual at any time.

5.2.2. The processing is necessary for the performance of a contract, to which the individual is a party, or is necessary for the purpose of taking steps with regards to entering into a contract with the individual, at their request.

5.2.3. The processing is necessary for the performance of a legal obligation to which we are subject.

5.2.4. The processing is necessary to protect the vital interests of the individual or another.

5.2.5. 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 us.

5.2.6. The processing is necessary for the legitimate interests of the Trust (where the processing is not for any tasks the Trust performs as a public authority) or a third party, provided the individual's rights and freedoms are not overridden.

6. CONDITIONS FOR PROCESSING IN THE SECOND DATA PROTECTION PRINCIPLE

6.1. In order to comply with the requirement for purposes of processing to be limited, data will be collected and processed in line with our Privacy Notices.

6.2. Where data is to be collected and/or processed in a way not addressed in our Privacy notices, additional details will be provided to explain the reasons for doing so.

6.3. The Trust will only use data for the purposes it is collected.

7. CONDITIONS FOR PROCESSING IN THE THIRD DATA PROTECTION PRINCIPLE

7.1. In order to comply with the principle of data minimisation, the Trust will collect, process, and dispose of data in accordance with the Records Retention Policy.

7.2. Data collected and processed will be adequate yet limited to what is necessary to fulfil the purpose of processing.

8. CONDITIONS FOR PROCESSING IN THE FOURTH DATA PROTECTION PRINCIPLE

8.1. In order to comply with the requirement for data to be accurate and up-to-date, the Trust will be responsible for checking the quality and accuracy of the personal data. This will be done via regular data collection processes.

8.2. Where an individual's personal data has changed, for example where contact details change, the individual is responsible for informing the Trust – more information about data rectification can be found in section 18 below.

9. CONDITIONS FOR PROCESSING IN THE FIFTH DATA PROTECTION PRINCIPLE

9.1. In order to comply with the requirement for data to be retained no longer than is necessary to fulfil it's purpose, the Trust will regularly review the records held to ensure that personal data is not held longer than necessary, and that is has been held in accordance with the Records Retention Policy.

9.2. The Trust will ensure that when personal data is authorised for disposal, it is done appropriately, in accordance with the Records Retention Policy.

10. CONDITIONS FOR PROCESSING IN THE SIXTH DATA PROTECTION PRINCIPLE

10.1. In order to comply with the principle of accountability and confidentiality, the Trust will ensure appropriate security measures to safeguard personal data whether it is held in paper files or on our computer system and follow the relevant security policy requirements at all times.

10.2. The Trust will take reasonable steps to ensure that members of staff will only have access to personal data where it is necessary for them to carry out their duties. All staff will be made aware of this policy and their duties under the GDPR.

10.3. The Trust will take reasonable steps to ensure that all personal information is held securely and is not accessible to unauthorised persons.

10.4. For further details as regards security of IT systems, please refer to the Acceptable Use of ICT Policy.

10.5. The Trust will share personal data with others only when it is necessary and legally appropriate to do so, in accordance with the Third Party Requests for Data policy.

11. CONDITIONS FOR PROCESSING IN THE SEVENTH DATA PROTECTION PRINCIPLE

11.1. In order to comply with the requirement of accountability, the Trust will ensure that all staff complete regular GDPR training, and that records of this training are retained.

11.2. The Trust will also retain records of GDPR matters and rights requests to evidence accountability, which will be regularly reported to Local Governing Bodies and the Trust Board.

12. USE OF PERSONAL DATA BY THE TRUST

12.1. The Trust processes personal data on pupils, staff and other individuals, such as visitors and job applicants. In each case, the personal data must be processed in accordance with the data protection principles as outlined in paragraph 3.1 above.

12.2. Pupils

12.2.1. The personal data held regarding pupils includes contact details, biometric data, assessment / examination results, attendance information, characteristics such as ethnic group, special educational needs, any relevant medical information, and photographs or video, including CCTV.

12.2.2. The data is used in order to support the education of the pupils, to monitor and report on their progress, to provide appropriate pastoral care, and to assess how well the Trust as a whole is doing, together with any other uses normally associated with this provision in a school environment.

12.2.3. The Trust may make use of limited personal data (such as contact details) relating to pupils, and their parents or guardians for fundraising, marketing or promotional purposes and to maintain relationships with pupils of the Trust, but only where consent has been provided to this.

12.2.4. In particular, the Trust may:

- transfer information to any association society or club set up for the purpose of maintaining contact with pupils or for fundraising, marketing or promotional purposes relating to the academy but only where consent has been obtained first;
- make personal data, including sensitive personal data, available to staff for planning curricular or extra-curricular activities;
- keep the pupil's previous school informed of his / her academic progress and achievements e.g. sending a copy of the school reports for the pupil's first year at a school within the Trust to their previous school;
- Use photographs of pupils in accordance with the photograph policy.

12.2.5. Any wish to limit or object to any use of personal data should be notified to the Data Protection Officer, and will be responded to appropriately in line with sections 15-23 below.

12.3. Staff

12.3.1. The personal data held about staff will include contact details, employment

history, information relating to career progression, employment references, information relating to DBS checks, absence records, disciplinary records, information relating to occupational pensions, photographs and videos, including CCTV.

12.3.2. The data is used to comply with legal obligations placed on the Trust in relation to employment, and the education and safeguarding of children in a school environment. The Trust may pass information to other regulatory authorities where appropriate and may use names and photographs of staff in publicity and promotional material. Personal data will also be used when giving references.

12.3.3. Staff should note that information about disciplinary action may be kept for longer than the duration of the sanction. Although treated as "spent" once the period of the sanction has expired, the details of the incident may need to be kept for a longer period, for example where safeguarding rules require this.

12.3.4. Any wish to limit or object to any use of personal data should be notified to the Data Protection Officer, and will be responded to appropriately in line with sections 20 & 22 below.

12.4. Information relating to DBS checks:

12.4.1. DBS checks are carried out on the basis of the Trust's legal obligations in relation to the safer recruitment of staff as stipulated in the Independent School Standards Regulations, and the DBS information (which will include personal data

12.4.2. relating to criminal convictions and offences) is further processed in the substantial public interest, with the objective of safeguarding children. Retention of the information is covered by the Records Retention Policy.

12.4.3. Access to the DBS information is restricted to those staff who have a genuine need to have access to it for their job roles. In addition to the provisions of the GDPR and the Data Protection Act 2018, disclosure of this information is restricted by section 124 of the Police Act 1997 and disclosure to third parties will only be made if it is determined to be lawful.

12.5. Other Individuals

12.5.1. The Trust may hold personal information in relation to other individuals who have contact with the school, including but not limited to, volunteers, job applicants and guests. Such information shall be held only in accordance with the data protection principles and shall not be kept longer than necessary.

13. DISCLOSURE OF PERSONAL DATA TO THIRD PARTIES

13.1. The Trust may receive requests from third parties (i.e. those other than the data subject, the Trust, and employees of the Trust) to disclose personal data it holds about pupils, their parents or guardians, staff or other individuals. This information will not generally be disclosed unless one of the specific exemptions under data protection legislation which allow disclosure applies; or where necessary for the legitimate interests of the requestor concerned or the Trust.

13.2. Information about the disclosure of data to third parties, can be found in the Third Party Data Request policy.

14. CONFIDENTIALITY OF PUPIL CONCERNS

14.1. Where a pupil seeks to raise concerns confidentially with a member of staff and expressly withholds their agreement to their personal data being disclosed to their parents or guardian, the Trust will maintain confidentiality unless it has reasonable grounds to believe that the pupil does not fully understand the consequences of withholding their consent, or where the Trust believes disclosure will be in the best interests of the pupil or other pupils. Disclosure for a safeguarding purpose will be lawful because it will be in the substantial public interest.

15. DATA SUBJECT RIGHTS

15.1. The Trust has an obligation to comply with the rights of individuals under the UK General Data Protection Regulations and takes these rights seriously. These rights are:

- The right to be informed
- The right of access
- The right to rectification
- The right to erasure
- The right to restrict processing
- The right to data portability
- The right to object
- Rights relating to automated decision making and profiling.

15.2. Although data protection legislation affords these rights to individuals, in some cases, the obligations of the Trust to share data with other organisations, including but not limited to the Department for Education (DfE) and the Local Authority (LA) may override these rights. 15.3. Further information about this can be found in our Privacy Notices.

16. The right to be informed

16.1. 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 via the Trust website (https://wwww.unitysp.co.uk) and free of charge.

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

16.3. 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.

17. The right of access

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

17.2. 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.

17.3. Further information about the right of access, including how to make a subject access request can be found in our Subject Access Request policy.

18. The right to rectification

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

18.2. Where the personal data in question has been disclosed to third parties, the school will inform them of the rectification unless it is impossible or involves disproportionate effort to do so.

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

18.4. Where no action is being taken in response to a request for rectification, the school 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.

19. The right to erasure

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

19.2. 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 data is processed on the basis of consent, and 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

19.3. The Trust 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 defense of legal claims

19.4. 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.

19.5. 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.

19.6. The Trust will respond to any requests for erasure within one month.

19.7. 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.

20. The right to restrict processing

20.1. Individuals have the right to block or suppress the Trust's processing of personal data.

20.2. In the event that processing is restricted, the Trust 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.

20.3. The Trust will restrict the processing of personal data in the following circumstances:

20.4. Where an individual contests the accuracy of the personal data, processing will be restricted until the Trust has verified the accuracy of the data

20.5. Where an individual has objected to the processing and the Trust is considering whether their legitimate grounds override those of the individual

20.6. Where processing is unlawful and the individual opposes erasure and requests restriction instead

20.7. Where the school no longer needs the personal data but the individual requires the data to establish, exercise or defend a legal claim

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

20.9. The Trust will inform individuals when a restriction on processing has been lifted.

21. The right to data portability

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

21.2. 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.

21.3. 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

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

21.5. The Trust will provide the information free of charge.

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

the individual.

21.7. Unity Schools Partnership is not required to adopt or maintain processing systems which are technically compatible with other organisations.

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

21.9. The Trust will respond to any requests for portability within one month.

21.10. 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.

21.11. Where no action is being taken in response to a request, the Trust 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.

22. The right to object

22.1. The Trust 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.

22.2. 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.

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

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

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

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

22.4.1. The Trust will stop processing personal data for direct marketing purposes as soon as an objection is received.

22.4.2. The Trust cannot refuse an individual's objection regarding data that is being processed for direct marketing purposes.

22.5. Where personal data is processed for research purposes:

22.5.1. The individual must have grounds relating to their particular situation in order to exercise their right to object.

22.6. Where the processing of personal data is necessary for the performance of a public interest task, the Trust is not required to comply with an objection to the processing of the data.

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

23. Rights related to automated decision making and profiling.

23.1. Automated decision making is the use of computer algorithms to make decisions based on existing data, without any human involvement. Profiling is the automated processing and analysis of personal data to evaluate and categorise individuals.

23.2. Unity Schools Partnership and the academies therein do not use any methods of

automated decision making or profiling.

24. BIOMETRIC RECOGNITION SYSTEMS.

24.1. Where we use pupils' biometric data as part of an automated biometric recognition system (for example, where pupils use fingerprints to receive school dinners instead of paying with cash, we will comply with the requirements of the Protection of Freedoms Act 2012.

24.2. Any enquiries about the biometric recognition systems should be directed to the Data Protection Officer in the first instance.

24.3. Further information about the Trust's use of biometric recognition systems can be found in the Biometric Data Policy.

25. CCTV

25.1. We use CCTV in various locations across the Trust to ensure safety. We will adhere to the ICO's (Information Commissioner's Office) code of practice for the use of CCTV.

25.2. Any enquiries about CCTV systems should be directed to the Data Protection Officer in the first instance.

25.3. Further information about the Trust's use of CCTV can be found in the CCTV policy.

26. BREACH OF ANY REQUIREMENT OF THE GDPR

26.1. Any and all breaches of the GDPR, including a breach of any of the data protection principles shall be reported as soon as it is/they are discovered, to the Data Protection Officer.

26.1.1. For breaches reported within one of the Trust's schools, this should be done via the Data Protection Lead.

26.2. Once notified, the Data Protection Officer shall assess:

- the extent of the breach;
- the risks to the data subjects as a consequence of the breach;
- any security measures in place that will protect the information;
- any measures that can be taken immediately to mitigate the risk to the individuals.

26.3. Unless the Data Protection Officer concludes that there is unlikely to be any risk to individuals from the breach, it must be notified to the Information Commissioner's Office within 72 hours of the breach having come to the attention of the Trust, unless a delay can be justified.

26.4. The Information Commissioner shall be told:

- details of the breach, including the volume of data at risk, and the number and categories of data subjects;
- the contact point for any enquiries (which shall usually be the Data Protection Officer);

- the likely consequences of the breach;
- measures proposed or already taken to address the breach.

26.5. If the breach is likely to result in a high risk to the rights and freedoms of the affected individuals then the Data Protection Officer shall ensure that data subjects are notified of the breach without undue delay unless the data would be unintelligible to those not authorised to access it, or measures have been taken to mitigate any risk to the affected individuals.

26.6. Data subjects shall be told:

- the nature of the breach;
- who to contact with any questions;
- measures taken to mitigate any risks.

26.7. The Data Protection Officer shall then be responsible for instigating an investigation into the breach, including how it happened, and whether it could have been prevented. Any recommendations for further training or a change in procedure shall be reviewed by the board and a decision made about implementation of those recommendations.

27. CONTACT

27.1. If anyone has any concerns or questions in relation to this policy or any details herein, they should contact the Data Protection Officer.

27.2. The Data Protection Officer can be contacted via email: dpo@unitysp.co.uk

28. COMPLAINTS

28.1. If anyone has any concerns or questions in relation to this policy they should contact the Data Protection Officer.

28.2. The Data Protection Officer can be contacted via email: dpo@unitysp.co.uk