The 3-18 Education Trust

Data Protection Policy

'Every individual is in a great school.'

For Review: **Autumn Term 2025**
Review: **Autumn Term 2026**

www.3-18education.co.uk

Our Mission

To celebrate the diverse nature, culture and identity of our individual schools, whilst collaborating and enjoying the benefit of the team.

Our Values

Compassionate

To show care and understanding towards others.

Accomplished

To provide high quality education and training for all.

Resilient

To be solution focused and able to intelligently manage challenges.

The 3-18 Education Trust
101 Longden Road
Shrewsbury
SY3 9PS

Company Number: 08064698

Policy Monitoring and Review

Monitoring

The Chief Executive Officer will monitor the outcomes and impact of this policy on an annual basis.

Review

Member of Staff Responsible	Chief Executive Officer
Relevant Guidance/Advice/Legal Reference	The Data Protection, Privacy and Electronic Communications (Amendments etc) (EU Exit) Regulations 2020 Data Protection Act 2018 (DPA 2018) Protection of Freedoms Act 2012
Policy Adopted By	Board of Trustees
Consultation	Local Governing Bodies
Date of Policy	Autumn Term 2025
Review Period	Annually
Date of Next Review	Autumn Term 2026

Contents

1. Introduction 6
2. Definitions 6
Personal data 6
Special Category Data 6
Data Subject 6
Data Controller 6
Information Commissioner's Office 7
Processing 7
Automated Processing 7
Data Protection Impact Assessment (DPIA) 7
Criminal Records Information 7
3. When can the School Process Personal Data? 7
Data Protection Principles 7
Principle 1: Personal data must be processed lawfully, fairly and in a transparent manner. 7
Personal Data 8
Special Category Data 8
Consent 9
Principle 2: Personal data must be collected only for specified, explicit and legitimate purposes. 9
Principle 3: Personal data must be adequate, relevant and limited to what is necessary in relation to the purposes for which it is processed. 9
Principle 4: Personal data must be accurate and, where necessary, kept up to date. 9
Principle 5: Personal data must not be kept in a form which permits identification of data subjects for longer than is necessary for the purposes for which the data is processed 10
Principle 6: Personal data must be processed in a manner that ensures its security using appropriate technical and organisational measures to protect against unauthorised or unlawful processing and against accidental loss, destruction or damage. 10
Sharing Personal Data 10
Transfer of Data Outside the European Economic Area (EEA) 11
Transfer of Data Outside the UK 11
4. Data Subject's Rights and Requests 11
Biometric Recognition Systems. 12
Closed Circuit Television, Video Cameras (CCTV) 13
Photographs and Videos 13
Direct Marketing 14
Employee Obligations 14
Accountability 14

Data Protection Officer (DPO) 14
Personal Data Breaches 15
Transparency and Privacy Notices 15
Privacy by Design 16
Data Protection Impact Assessments (DPIAs) 16
Record Keeping 17
Training 17
Audit 17
Appendix A – Subject Access Requests 18
How to Recognise a Subject Access Request 18
How to Make a Data Subject Access Request 18
What to do When a Data Subject Access Request is Received 19
Acknowledging the Request 19
Verifying the Identity of a Requester or Requesting Clarification of the Request 19
Requests Made by Third Parties or on Behalf of Children 19
Fee for Responding to a SAR 20
Time Period for Responding to a SAR 21
School Closure Periods 21
Information to be Provided in Response to a Request 21
How to Locate Information 22
Protection of Third Parties - Exemptions to the Right of Subject Access 22
Other Exemptions to the Right of Subject Access 23
Crime detection and prevention 23
Confidential references 23
Legal professional privilege 24
Management forecasting 24
Negotiations 24
Refusing to Respond to a Request 24
Record Keeping 24
Appendix B – Online Links and Form to Make a Subject Access Request 25

1. Introduction

1.1. The UK General Data Protection Regulation (UK GDPR) ensures a balance between an individual's rights to privacy and the lawful processing of personal data undertaken by organisations in the course of their business. It aims to protect the rights of individuals about whom data is obtained, stored, processed or supplied and requires that organisations take appropriate security measures against unauthorised access, alteration, disclosure or destruction of personal data.

1.2. The 3-18 Education Trust (Trust) will protect and maintain a balance between data protection rights in accordance with the UK GDPR. This policy sets out how the Trust handles the personal data of pupils, parents, suppliers, employees, workers and other third parties.

1.3. This policy does not form part of any individual's terms and conditions of employment with the Trust and is not intended to have contractual effect. Changes to data protection legislation will be monitored and further amendments may be required to this policy in order to remain compliant with legal obligations.

1.4. All members of staff are required to familiarise themselves with its content and comply with the provisions contained in it. Breach of this policy may be treated as a disciplinary offence which may result in disciplinary action under the Trust's Disciplinary Policy and Procedure up to and including summary dismissal depending on the seriousness of the breach.

2. Definitions

Personal data

2.1. Personal data is any information relating to an individual where the individual can be identified (directly or indirectly) from that data alone or in combination with other identifiers the Trust possesses or can reasonably access. This includes special category data and pseudonymised personal data but excludes anonymous data or data that has had the identity of an individual permanently removed.

2.2. Personal data can be factual (for example, a name, email address, location or date of birth) or an opinion about that person's actions or behaviour.

2.3. Personal data will be stored either electronically or as part of a structured manual filing system in such a way that it can be retrieved automatically by reference to the individual or criteria relating to that individual.

Special Category Data

2.4. Previously termed "Sensitive Personal Data", Special Category Data is similar by definition and refers to data concerning an individual Data Subject's racial or ethnic origin, political or religious beliefs, trade union membership, physical and mental health, sexuality, biometric or genetic data and personal data relating to criminal offences and convictions.

Data Subject

2.5. An individual about whom such information is stored is known as the Data Subject. It includes but is not limited to employees.

Data Controller

2.6. The organisation storing and controlling such information (i.e., the Trust) is referred to as the Data Controller.

Information Commissioner's Office

2.7. The Information Commissioner's Office (ICO) upholds information rights in the public interest, promoting openness by public bodies and data privacy for individuals. ICO is an executive non-departmental public body, sponsored by the Department for Science, Innovation and Technology.

Processing

2.8. Processing data involves any activity that involves the use of personal data. This includes but is not limited to: obtaining, recording or holding data or carrying out any operation or set of operations on that data such as organisation, amending, retrieving, using, disclosing, erasing or destroying it. Processing also includes transmitting or transferring personal data to third parties.

Automated Processing

2.9. Any form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to an individual, in particular to analyse or predict aspects concerning that individual's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements.

2.10. An example of automated processing includes profiling and automated decision making. Automatic decision making is when a decision is made which is based solely on automated processing (without human intervention) which produces legal effects or significantly affects an individual. Automated decision making is prohibited except in exceptional circumstances.

Data Protection Impact Assessment (DPIA)

2.11. DPIAs are a tool used to identify risks in data processing activities with a view to reducing them.

Criminal Records Information

2.12. This refers to personal information relating to criminal convictions and offences, allegations, proceedings, and related security measures.

3. When can the School Process Personal Data?

Data Protection Principles

3.1. The Trust adheres to the principles relating to the processing of personal data as set out in the UK GDPR. The principles are set out below.

Principle 1: Personal data must be processed lawfully, fairly and in a transparent manner.

3.2. The Trust only collect, process and share personal data fairly and lawfully and for specified purposes. The Trust must have a specified purpose for processing personal data and special category data as set out in the UK GDPR.

3.3. Before the processing starts for the first time, the Trust will review the purposes of the particular processing activity and select the most appropriate lawful basis for that processing. The Trust will then regularly review those purposes whilst processing continues in order to satisfy that the processing is necessary for the purpose of the relevant lawful basis (i.e., that there is no other reasonable way to achieve that purpose).

Personal Data

3.4. The Trust may only process a data subject's personal data if one of the following fair processing conditions are met:

- The data subject has given their consent.
- The processing is necessary for the performance of a contract with the data subject or for taking steps at their request to enter into a contract.
- To protect the data subject's vital interests.
- To meet our legal compliance obligations (other than a contractual obligation).
- To perform a task in the public interest or in order to carry out official functions as authorised by law.
- For the purposes of the Trust's legitimate interests where authorised in accordance with data protection legislation. This is provided that it would not prejudice the rights and freedoms or legitimate interests of the data subject.

Special Category Data

3.5. The Trust may only process special category data if it is entitled to process personal data (using one of the fair processing conditions above) AND one of the following conditions are met: -

- The data subject has given their explicit consent.
- The processing is necessary for the purposes of exercising or performing any right or obligation which is conferred or imposed on the Trust in the field of employment law, social security law or social protection law. This may include, but is not limited to, dealing with sickness absence, dealing with disability and making adjustments for the same, arranging private health care insurance and providing contractual sick pay.
- To protect the data subject's vital interests.
- To meet the Trust's legal compliance obligations (other than a contractual obligation).
- Where the data has been made public by the data subject.
- To perform a task in the substantial public interest or in order to carry out official functions as authorised by law.
- Where it is necessary for the purposes of preventive or occupational medicine, for the assessment of the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment or the management of health or social care systems and services.
- Where it is necessary for reasons of public interest in the area of public health.
- The processing is necessary for archiving, statistical or research purposes.

3.6. The Trust identifies and documents the legal grounds being relied upon for each processing activity.

Consent

3.7. Where the Trust relies on consent as a fair condition for processing (as set out above), it will adhere to the requirements set out in the UK GDPR.

3.8. Consent must be freely given, specific, informed and be an unambiguous indication of the data subject's wishes by which they signify agreement to the processing of personal data relating to them. Explicit consent requires a very clear and specific statement to be relied upon (i.e. more than just mere action is required).

3.9. A data subject will have consented to processing of their personal data if they indicate agreement clearly either by a statement or positive action to the processing. Consent requires affirmative action so silence, pre-ticked boxes or inactivity will not amount to valid consent.

3.10. Data subjects must be easily able to withdraw consent to processing at any time and withdrawal must be promptly honoured.

3.11. If explicit consent is required, the Trust will normally seek another legal basis to process that data. However, if explicit consent is required, the data subject will be provided with full information in order to provide explicit consent.

3.12. The Trust will keep records of consents obtained in order to demonstrate compliance with consent requirements under the UK GDPR.

Principle 2: Personal data must be collected only for specified, explicit and legitimate purposes.

3.13. Personal data will not be processed in any matter that is incompatible with the legitimate purposes.

3.14. The Trust will not use personal data for new, different or incompatible purposes from that disclosed when it was first obtained unless it has informed the data subject of the new purpose (and they have consented where necessary).

Principle 3: Personal data must be adequate, relevant and limited to what is necessary in relation to the purposes for which it is processed.

3.15. The Trust will only process personal data when its obligations and duties require it to do so. The Trust will not collect excessive data and ensure any personal data collected is adequate and relevant for the intended purposes.

3.16. When personal data is no longer needed for specified purposes, the Trust shall delete or anonymise the data. Please refer to the Trust's Records Management Policy for further guidance.

Principle 4: Personal data must be accurate and, where necessary, kept up to date.

3.17. The Trust will endeavour to correct or delete any inaccurate data being processed by checking the accuracy of the personal data at the point of collection and at regular intervals afterwards. The Trust will take all reasonable steps to destroy or amend inaccurate or out of date personal data.

3.18. Data subjects also have an obligation to ensure that their data is accurate, complete, up to date and relevant. Data subjects have the right to request rectification to incomplete or inaccurate data held by the Trust.

Principle 5: Personal data must not be kept in a form which permits identification of data subjects for longer than is necessary for the purposes for which the data is processed.

3.19. Legitimate purposes for which the data is being processed may include satisfying legal, accounting or reporting requirements. The Trust will ensure that they adhere to legal timeframes for retaining data.

3.20. The Trust will take reasonable steps to destroy or erase from its systems all personal data that is no longer require. The Trust will also ensure that data subjects are informed of the period for which data is stored and how that period is determined in the Trust's privacy notices.

3.21. Please refer to the Trust's Records Management Policy for further details about how the Trust retains and removes data.

Principle 6: Personal data must be processed in a manner that ensures its security using appropriate technical and organisational measures to protect against unauthorised or unlawful processing and against accidental loss, destruction or damage.

3.22. In order to assure the protection of all data being processed, the Trust will develop, implement and maintain reasonable safeguard and security measures. This includes using measures such as:

- Encryption.
- Pseudonymisation (this is where the Trust replaces information that directly or indirectly identifies an individual with one or more artificial identifiers or pseudonyms so that the person to whom the data relates cannot be identified without the use of additional information which is meant to be kept separately and secure).
- Ensuring authorised access on both hard copy and electronic files (i.e. that only people who have a need to know the personal data are authorised to access it).
- Adhering to confidentiality principles.
- Ensuring personal data is accurate and suitable for the process for which it is processed.

3.23. The Trust follow procedures and technologies to ensure security and will regularly evaluate and test the effectiveness of those safeguards to ensure security in processing personal data.

3.24. The Trust will only transfer personal data to third party service providers who agree to comply with the required policies and procedures and agree to put adequate measures in place.

3.25. Full details on the Trust's security measures are set out in the Trust's Information Security Policy and Procedure.

Sharing Personal Data

3.26. The Trust will generally not share personal data with third parties unless certain safeguards and contractual arrangements have been put in place. The following points will be considered:

- Whether the third party has a need to know the information for the purposes of providing the contracted services.
- Whether sharing the personal data complies with the privacy notice that has been provided to the data subject and, if required, the data subject's consent has been obtained.
- Whether the third party has agreed to comply with the required data security standards, policies and procedures and implemented adequate security measures.
- Whether the transfer complies with any applicable cross border transfer restrictions; and
- Whether a fully executed written contract that contains UK GDPR approved third party clauses has been obtained.

3.27. There may be circumstances where the Trust is required either by law or in the best interests of pupils, parents or staff to pass information onto external authorities for example, the Local Authority, Ofsted or the department of health. These authorities are up to date with data protection law and have their own policies relating to the protection of any data that they receive or collect.

3.28. The intention to share data relating to individuals to an organisation outside of the Trust shall be clearly defined within written notifications including details and the basis for sharing the data.

Transfer of Data Outside the European Economic Area (EEA)

3.29. The UK GDPR restricts data transfers to countries outside the EEA in order to ensure that the level of data protection afforded to individuals by the UK GDPR is not undermined.

3.30. The Trust will not transfer data to another country outside of the EEA without appropriate safeguards being in place and in compliance with the UK GDPR. All staff must comply with the Trust's guidelines on transferring data outside of the EEA. For the avoidance of doubt, a transfer of data to another country can occur when the Trust transmits, sends, views or accesses that data in that particular country.

Transfer of Data Outside the UK

3.31. The Trust may transfer personal information outside the UK and/or to international organisations on the basis that the country, territory or organisation is designated as having an adequate level of protection. Alternatively, the organisation receiving the information has provided adequate safeguards by way of binding corporate rules, Standard Contractual Clauses or compliance with an approved code of conduct.

4. Data Subject's Rights and Requests

4.1. Personal data must be made available to data subjects as set out within this policy and data subjects must be allowed to exercise certain rights in relation to their personal data.

4.2. The rights data subjects have in relation to how the Trust handles their personal data are set out below:

- (Where consent is relied upon as a condition of processing) To withdraw consent to processing at any time.
- Receive certain information about the Trust's processing activities.
- Request access to their personal data that the Trust holds (see "Subject Access Requests" at Appendix 1).
- Prevent the Trust's use of their personal data for marketing purposes.
- Ask the Trust to erase personal data if it is no longer necessary in relation to the purposes for which it was collected or processed or to rectify inaccurate data or to complete incomplete data.
- Restrict processing in specific circumstances.
- Challenge processing which has been justified on the basis of the Trust's legitimate interests or in the public interest.
- Request a copy of an agreement under which personal data is transferred outside of the EEA.
- Object to decisions based solely on automated processing.
- Prevent processing that is likely to cause damage or distress to the data subject or anyone else.
- Be notified of a personal data breach which is likely to result in high risk to their rights and freedoms.
- Make a complaint to the supervisory authority.
- In limited circumstances, receive or ask for their personal data to be transferred to a third party in a structured, commonly used and machine-readable format.

4.3. If any request is made to exercise the rights above, it is a requirement for the relevant staff member within the Trust to verify the identity of the individual making the request. Please see Appendix B for details.

Biometric Recognition Systems.

4.4. In some of the Trust's Schools pupils' biometric data is used as part of an automated biometric recognition system (for example, pupils may use fingerprints to receive school dinners instead of paying with cash). The Trust complies with the requirements of the Protection of Freedoms Act 2012.

4.5. Parents/carers will be notified before any biometric recognition system is put in place or before their child first takes part in it. The school must receive written consent from at least one parent or carer before any biometric data is taken from their child and first process it.

4.6. Parents/carers and pupils have the right to choose not to use the School's biometric system(s). The Trust will provide alternative means of accessing the relevant services for those pupils.

4.7. Parents/carers and pupils can object to participation in the School's biometric recognition system(s), or withdraw consent, at any time, and the Trust will make sure that any relevant data already captured is deleted.

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

4.9. Full details are set out in the Trust's Protection of Pupils' Biometric Information and Consent to Use Biometric Data document.

4.10. Where staff members or other adults use the school's biometric system(s), the Trust 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.

Closed Circuit Television, Video Cameras (CCTV)

4.11. The Trust uses CCTV in various locations around some school sites for surveillance (the act of watching a person or a place). The purpose of the Trust's CCTV system is to:

- Make members of the school community feel safe.
- Protect members of the school community from harm to themselves or to their property.
- Deter criminality in the Trust's sites.
- Protect Trust assets and buildings.
- Assist police to deter and detect crime.
- Determine the cause of accidents.
- Assist in the effective resolution of any disputes which may arise in the course of disciplinary and grievance proceedings.
- To assist in the defence of any litigation proceedings.

4.12. The CCTV system will not be used to:

- Encroach on an individual's right to privacy.
- Follow particular individuals, unless there is an ongoing emergency incident occurring.
- Pursue any other purposes than the ones stated above.

4.13. The list of uses of CCTV is not exhaustive and other purposes may be or become relevant.

4.14. CCTV cameras are installed in such a way that they are not hidden from view. Signs are predominantly displayed where relevant so that staff, students, visitors and members of the public are made aware that they are entering an area covered by CCTV. The signs also contain contact details as well as a statement of purposes for which CCTV is used.

4.15. The Trust will follow the ICO's code of practice for the use of CCTV. Full details on the Trust's management of CCTV are set out in the Trust's Operation of CCTV Procedure.

Photographs and Videos

4.16. As part of school activities, photographs and record images of individuals within our schools may be taken. Each School will obtain written consent from parents/carers for photographs and videos to be taken of their child for communication, marketing and promotional materials. It will be clearly explained how the photograph and/or video will be used to both the parent/carer and pupil. Uses may include:

- Within school on notice boards and in school magazines, brochures, newsletters, etc.
- Outside of school by external agencies such as the school photographer, newspapers, campaigns.

- Online on our school and trust website or social media pages.

4.17. Consent can be refused or withdrawn at any time. If consent is withdrawn, the photograph or video will be deleted and not distributed further.

4.18. When using photographs and videos in this way they will not be accompanied with any other personal information about the child, to ensure they cannot be identified.

Direct Marketing

4.19. The Trust is subject to certain rules and privacy laws when marketing. For example, a data subject's prior consent will be required for electronic direct marketing (for example, by email, text or automated calls).

4.20. The Trust will explicitly offer individuals the opportunity to object to direct marketing and will do so in an intelligible format which is clear for the individual to understand. The Trust will promptly respond to any individual objection to direct marketing.

Employee Obligations

4.21. Employees may have access to the personal data of other members of staff, suppliers, parents or pupils of the Trust in the course of their employment or engagement. If so, the Trust expects those employees to help meet the Trust's data protection obligations to those individuals. Specifically, employees must: -

- Only access the personal data that they have authority to access, and only for authorised purposes, confidentiality is expected at all times.
- Only allow others to access personal data if they have appropriate authorisation.
- Keep personal data secure for example, by complying with rules on access to school premises, computer access, password protection and secure file storage and destruction Please refer to the Trust's Information Security Policy and Procedure for further details about the Trust's security processes.
- Not remove personal data or devices containing personal data from the Trust's premises unless appropriate security measures are in place (such as pseudonymisation, encryption, password protection) to secure the information.
- Not store personal information on local drives.

Accountability

4.22. The Trust will ensure compliance with data protection principles by implementing appropriate technical and organisational measures. The Trust is responsible for and demonstrates accountability with the UK GDPR principles.

Data Protection Officer (DPO)

4.23. Please find below details of the Trust's Data Protection Officer: -

Data Protection Officer: Judicium Consulting Limited
Address: 5th Floor, 98 Theobalds Road, London, WC1X 8WB
Email: dataservices@judicium.com
Web: www.judiciumeducation.co.uk

Telephone: 0345 548 7000 option 1 then option 1 again

4.24. Please contact the DPO with any questions about the operation of this Data Protection Policy or the UK GDPR or if there are any concerns that this policy is not being or has not been followed. In particular, the DPO must always be contacted in the following circumstances:

- If there is uncertainty of the lawful basis being relied on by the Trust to process personal data.
- If consent is being relied on as a fair reason for processing (please see below the section on consent for further detail);
- If there is uncertainty about the retention periods for the personal data being processed but refer to the Trust's Data Retention Policy in the first instance.
- If there is uncertainty about what security measures need to be put in place to protect personal data.
- If there has been a personal data breach processed but refer to the Trust's Data Breach Policy in the first instance.
- If there is uncertainty on what basis to transfer personal data outside the EEA.
- If assistance is needed when dealing with any rights invoked by a data subject.
- Whenever there is a significant new (or a change in) processing activity which is likely to require a data protection impact assessment or if there are plans to use personal data for purposes other than what it was collected for.
- If there are plans to undertake any activities involving automated processing or automated decision making.
- If assistance is needed to comply with applicable law when carrying out direct marketing activities.
- If assistance is needed with any contracts or other areas in relation to sharing personal data with third parties.

Personal Data Breaches

4.25. The UK GDPR requires the Trust to notify any applicable personal data breach to the ICO.

4.26. The Trust has put in place procedures to deal with any suspected personal data breach and will notify data subjects or any applicable regulator where the Trust is legally required to do so.

4.27. If this is or there is concern that a personal data breach has occurred, individuals must not attempt to investigate the matter. Immediately contact the Trust's IT Director or the Trust's DPO.

4.28. Full details are set out in the Trust's Data Breach Procedure.

Transparency and Privacy Notices

4.29. The Trust will provide detailed, specific information to data subjects. This information will be provided through the Trust's privacy notices which are concise, transparent, intelligible, easily accessible and in clear and plain language so that a data

subject can easily understand them. The Trust's privacy notices are tailored to suit the data subject and set out information about how the Trust use their data.

4.30. Whenever the Trust collects personal data directly from data subjects, including for human resources or employment purposes, the Trust will provide the data subject with all the information required by the UK GDPR. This includes the identity of the Data Protection Officer, the Trust's contact details, how and why the Trust will use, process, disclose, protect and retain personal data. This information will be provided within the Trust's Privacy Notices.

4.31. When personal data is collected indirectly (for example, from a third party or a publicly available source), where appropriate, the Trust will provide the data subject with the above information as soon as possible after receiving the data. The Trust will also confirm whether that third party has collected and processed data in accordance with the UK GDPR.

4.32. Notifications shall be in accordance with ICO guidance and where relevant, be written in a form understandable by those defined as "children" under the UK GDPR.

Privacy by Design

4.33. The Trust adopt a privacy by design approach to data protection to ensure that the Trust adheres to data compliance and to implement technical and organisational measures in an effective manner.

4.34. Privacy by design is an approach that promotes privacy and data protection compliance from the start. To help achieve this, the Trust takes into account the nature and purposes of the processing, any cost of implementation and any risks to rights and freedoms of data subjects when implementing data processes.

Data Protection Impact Assessments (DPIAs)

4.35. In order to achieve a privacy by design approach, the Trust conduct DPIAs for any new technologies or programmes being used by the Trust which could affect the processing of personal data. In any event, the Trust carries out DPIAs when required by the UK GDPR in the following circumstances: -

- For the use of new technologies (programs, systems or processes) or changing technologies.
- For the use of automated processing.
- For large scale processing of special category data.
- For large scale, systematic monitoring of a publicly accessible area through the use of CCTV.

4.36. The Trust's DPIAs contain: -

- A description of the processing, its purposes and any legitimate interests used.
- An assessment of the necessity and proportionality of the processing in relation to its purpose.
- An assessment of the risk to individuals.
- The risk mitigation measures in place and demonstration of compliance.

Record Keeping

4.37. The Trust is required to keep full and accurate records of data processing activities. These records include: -

- The name and contact details of the Trust.
- The name and contact details of the Data Protection Officer.
- Descriptions of the types of personal data used.
- Description of the data subjects.
- Details of the Trust's processing activities and purposes.
- Details of any third party recipients of the personal data.
- Where personal data is stored.
- Retention periods.
- Security measures in place.

Training

4.38. The Trust will ensure all relevant personnel have undergone adequate training to enable them to comply with data privacy laws.

Audit

4.39. The Trust, through its Data Protection Officer regularly test the data systems and processes to assess compliance. These are done through data audits which take place annually to review use of personal data.

Appendix A – Subject Access Requests

Under Data Protection Law, data subjects have a general right to find out whether the Trust hold or process personal data about them, to access that data, and to be given supplementary information. This is known as the right of access or the right to make a data subject access request (SAR). The purpose of the right is to enable the individual to be aware of and verify the lawfulness of the processing of personal data that the Trust are undertaking.

This appendix provides guidance for staff members on how data subject access requests should be handled and for all individuals on how to make a SAR.

Failure to comply with the right of access under UK GDPR puts both staff and the Trust at potentially significant risk and so the Trust takes compliance with this policy very seriously.

A data subject has the right to be informed by the Trust of the following:

- Confirmation that their data is being processed.
- Access to their personal data.
- A description of the information that is being processed.
- The purpose for which the information is being processed.
- The recipients/class of recipients to whom that information is or may be disclosed.
- Details of the Trust's sources of information obtained.
- In relation to any personal data processed for the purposes of evaluating matters in relation to the data subject that has constituted or is likely to constitute the sole basis for any decision significantly affecting him or her, to be informed of the logic of the Data Controller's decision making. Such data may include, but is not limited to, performance at work, creditworthiness, reliability and conduct.
- Other supplementary information.

How to Recognise a Subject Access Request

A data subject access request is a request from an individual (or from someone acting with the authority of an individual, e.g., a solicitor or a parent making a request in relation to information relating to their child):

- for confirmation as to whether the Trust process personal data about him or her and, if so
- for access to that personal data
- and/or certain other supplementary information

A valid SAR can be both in writing (by letter, email, WhatsApp text) or verbally (e.g., during a telephone conversation). The request may refer to the UK GDPR and/or to 'data protection' and/or to 'personal data' but does not need to do so in order to be a valid request. For example, a letter which states 'please provide me with a copy of information that the Trust hold about me' would constitute a data subject access request and should be treated as such.

A data subject is generally only entitled to access their own personal data and not information relating to other people.

How to Make a Data Subject Access Request

Whilst there is no requirement to do so, the Trust encourage any individuals who wish to make such a request to make the request in writing, detailing exactly the personal data being requested. This allows the Trust to easily recognise that the requester wishes to make a data subject access

request and the nature of the request. If the request is unclear/vague the Trust may be required to clarify the scope of the request which may in turn delay the start of the time period for dealing with the request.

What to do When a Data Subject Access Request is Received
All data subject access requests should be immediately directed to the School's Business Manager who should contact Judicium as DPO in order to assist with the request and what is required. There are limited timescales within which the Trust must respond to a request and any delay could result in failing to meet those timescales, which could lead to enforcement action by the Information Commissioner's Office (ICO) and/or legal action by the affected individual.

Acknowledging the Request
When receiving a SAR the Trust shall acknowledge the request as soon as possible and inform the requester about the statutory deadline (of one calendar month) to respond to the request.

- In addition to acknowledging the request, the Trust may ask for:
- proof of ID (if needed);
- further clarification about the requested information;
- if it is not clear where the information shall be sent, the Trust must clarify what address/email address to use when sending the requested information; and/or
- consent (if requesting third party data).

The Trust should work with the DPO in order to create the acknowledgment.

Verifying the Identity of a Requester or Requesting Clarification of the Request
Before responding to a SAR, the Trust will take reasonable steps to verify the identity of the person making the request. In the case of current employees, this will usually be straightforward. The Trust is entitled to request additional information from a requester in order to verify whether the requester is in fact who they say they are. Where the Trust has reasonable doubts as to the identity of the individual making the request, evidence of identity may be established by production of a passport, driving license, a recent utility bill with current address, birth/marriage certificate, credit card or a mortgage statement.

If an individual is requesting a large amount of data the Trust may ask the requester for more information for the purpose of clarifying the request, but the requester shall never be asked why the request has been made. The Trust shall let the requester know as soon as possible where more information is needed before responding to the request.

In both cases, the period of responding begins when the additional information has been received. If the Trust do not receive this information, the Trust will be unable to comply with the request.

Requests Made by Third Parties or on Behalf of Children
The Trust need to be satisfied that the third party making the request is entitled to act on behalf of the individual, but it is the third party's responsibility to provide evidence of this entitlement. This might be a written authority to make the request, or it might be a more general power of attorney. The Trust may also require proof of identity in certain circumstances.

If the Trust is in any doubt or has any concerns as to providing the personal data of the data subject to the third party, then it should provide the information requested directly to the data subject. It is then a matter for the data subject to decide whether to share this information with any third party.

CCTV footage will only be shared with a third party to further the aims of the CCTV system set out in the section on CCTV (e.g. assisting the police in investigating a crime). Footage will only ever be shared with authorised personnel such as law enforcement agencies or other service providers who reasonably need access to the footage (e.g. investigators). The Trust will comply with any court orders that grant access to the CCTV footage. The Trust will provide the courts with the footage they need without giving them unrestricted access. The DPO will consider very carefully how much footage to disclose and seek legal advice if necessary.

When requests are made on behalf of children, it is important to note that even if a child is too young to understand the implications of subject access rights, it is still the right of the child, rather than of anyone else such as a parent or guardian, to have access to the child's personal data. Before responding to a SAR for information held about a child, the Trust should consider whether the child is mature enough to understand their rights. If the school is confident that the child can understand their rights, then the Trust should usually respond directly to the child or seek their consent before releasing their information.

It shall be assessed if the child is able to understand (in broad terms) what it means to make a subject access request and how to interpret the information they receive as a result of doing so. When considering borderline cases, it should be taken into account, among other things:

- the child's level of maturity and their ability to make decisions like this;
- the nature of the personal data;
- any court orders relating to parental access or responsibility that may apply;
- any duty of confidence owed to the child or young person;
- any consequences of allowing those with parental responsibility access to the child's or young person's information. This is particularly important if there have been allegations of abuse or ill treatment;
- any detriment to the child or young person if individuals with parental responsibility cannot access this information; and
- any views the child or young person has on whether their parents should have access to information about them.

Generally, a person aged 12 years or over is presumed to be of sufficient age and maturity to be able to exercise their right of access, unless the contrary is shown. In relation to a child 12 years of age or older, then provided that the School is confident that they understand their rights and there is no reason to believe that the child does not have the capacity to make a request on their own behalf, the Trust will require the written authorisation of the child before responding to the requester or provide the personal data directly to the child.

The Trust may also refuse to provide information to parents if there are consequences of allowing access to the child's information – for example, if it is likely to cause detriment to the child.

Fee for Responding to a SAR

The Trust will usually deal with a SAR free of charge. Where a request is considered to be manifestly unfounded or excessive a fee to cover administrative costs may be requested. If a request is considered to be manifestly unfounded or unreasonable the Trust will inform the requester why this is considered to be the case and that the Trust will charge a fee for complying with the request.

A fee may also be requested in relation to repeat requests for copies of the same information. In these circumstances a reasonable fee will be charged taking into account the administrative costs of providing the information.

If a fee is requested, the period of responding begins when the fee has been received.

Time Period for Responding to a SAR
The Trust has one calendar month to respond to a SAR. This will run from the day that the request was received or from the day when any additional identification or other information requested is received, or payment of any required fee has been received.

The circumstances where the Trust is in any reasonable doubt as to the identity of the requester, this period will not commence unless and until sufficient information has been provided by the requester as to their identity and in the case of a third party requester, the written authorisation of the data subject has been received.

The period for response may be extended by a further two calendar months in relation to complex requests. What constitutes a complex request will depend on the particular nature of the request. The DPO must always be consulted in determining whether a request is sufficiently complex as to extend the response period.

Where a request is considered to be sufficiently complex as to require an extension of the period for response, the Trust will need to notify the requester within one calendar month of receiving the request, together with reasons as to why this extension is considered necessary.

School Closure Periods
The Trust may not be able to respond to requests received during or just before school closure periods within the one calendar month response period. This is because the Trust/School will be closed. As a result, it is unlikely that the request will be able to be dealt with during this time. The Trust may not be able to acknowledge the request during this time (i.e., until a time when the Trust receive the request). However, if the Trust can acknowledge the request, it may still not be able to deal with it until the Trust re-opens. The Trust will endeavour to comply with requests as soon as possible and will keep in communication with the requester as far as possible. If the request is urgent, please provide the request during term times and not during/close to closure periods.

Information to be Provided in Response to a Request
The individual is entitled to receive access to the personal data the Trust process about him or her and the following information:

- the purpose for which the Trust process the data;
- the recipients or categories of recipient to whom the personal data has been or will be disclosed, in particular where those recipients are in third countries or international organisations;
- where possible, the period for which it is envisaged the personal data will be stored, or, if not possible, the criteria used to determine that period;
- the fact that the individual has the right:
    - to request that the Trust rectifies, erases or restricts the processing of his or her personal data; or

- to object to its processing;
- to lodge a complaint with the ICO;
- where the personal data has not been collected from the individual, any information available regarding the source of the data;
- any automated decision we have taken about him or her together with meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for him or her.

The information should be provided in a way that is concise, transparent, easy to understand and easy to access using clear and plain language, with any technical terms, abbreviations or codes explained. The response shall be given in writing if the SAR was made in writing in a commonly used electronic format.

The information that the Trust is required to supply in response to a SAR must be supplied by reference to the data in question at the time the request was received. However, as the Trust has one month in which to respond the Trust is allowed to take into account any amendment or deletion made to the personal data between the time the request is received and the time the personal data is supplied if such amendment or deletion would have been made regardless of the receipt of the SAR.

Therefore, the Trust is allowed to carry out regular housekeeping activities even if this means deleting or amending personal data after the receipt of a SAR. The Trust is not allowed to amend or delete data to avoid supplying the data.

How to Locate Information
The personal data the Trust need to provide in response to a data subject access request may be located in several of the electronic and manual filing systems. This is why it is important to identify at the outset the type of information requested so that the search can be focused.

Depending on the type of information requested, the Trust may need to search all or some of the following:

- Electronic systems, e.g., databases, networked and non-networked computers, servers, customer records, human resources system, email data, back up data, CCTV.
- Manual filing systems in which personal data is accessible according to specific criteria, e.g., chronologically ordered sets of manual records containing personal data.
- Data systems held externally by our data processors.
- Occupational health records.
- Pensions data.
- Share scheme information.
- Insurance benefit information.

The Trust should search these systems using the individual's name, employee number or other personal identifier as a search determinant.

Protection of Third Parties - Exemptions to the Right of Subject Access
There are circumstances where information can be withheld pursuant to a SAR. These specific exemptions and requests should be considered on a case by case basis.

The Trust will consider whether it is possible to redact information so that this does not identify those third parties. If their data cannot be redacted (for example, after redaction it is still obvious who the data relates to) then the Trust do not have to disclose personal data to the extent that doing so would involve disclosing information relating to another individual (including information identifying the other individual as the source of information) who can be identified from the information unless:

- the other individual has consented to the disclosure; or
- it is reasonable to comply with the request without that individual's consent.
- In determining whether it is reasonable to disclose the information without the individual's consent, all of the relevant circumstances will be taken into account, including:
- the type of information that they would disclose;
- any duty of confidentiality they owe to the other individual;
- any steps taken to seek consent from the other individual;
- whether the other individual is capable of giving consent; and
- any express refusal of consent by the other individual.

It needs to be decided whether it is appropriate to disclose the information in each case. This decision will involve balancing the data subject's right of access against the other individual's rights. If the other person consents to the Trust disclosing the information about them, then it would be unreasonable not to do so. However, if there is no such consent, the Trust must decide whether to disclose the information anyway. If there are any concerns in this regard, then the DPO should be consulted.

With respect to CCTV data/footage on occasion the Trust will reserve the right to refuse a SAR, if, for example, the release of the footage to the subject would prejudice an ongoing investigation.

Images that may identify other individuals need to be obscured to prevent unwarranted identification. The Trust will attempt to conceal their identities by blurring out their faces, or redacting parts of the footage. If this is not possible the Trust will seek their consent before releasing the footage. If consent is not forthcoming the still images may be released instead.

Footage that is disclosed in a SAR will be disclosed securely to ensure only the intended recipient has access to it.

Other Exemptions to the Right of Subject Access
In certain circumstances the Trust may be exempt from providing some or all of the personal data requested. These exemptions are described below and should only be applied on a case-by-case basis after a careful consideration of all the facts.

Crime detection and prevention
The Trust do not have to disclose any personal data being processed for the purposes of preventing or detecting crime; apprehending or prosecuting offenders; or assessing or collecting any tax or duty.

Confidential references
The Trust do not have to disclose any confidential references given to third parties for the purpose of actual or prospective:

- education, training or employment of the individual;
- appointment of the individual to any office; or
- provision by the individual of any service

This exemption does not apply to confidential references that the Trust receive from third parties. However, in this situation, granting access to the reference may disclose the personal data of another individual (i.e., the person giving the reference), which means that the School must consider the rules regarding disclosure of third-party data set out above before disclosing the reference.

Legal professional privilege
The Trust do not have to disclose any personal data which is subject to legal professional privilege.

Management forecasting
The Trust do not have to disclose any personal data processed for the purposes of management forecasting or management planning to assist us in the conduct of any business or any other activity.

Negotiations
The Trust do not have to disclose any personal data consisting of records of intentions in relation to any negotiations with the individual where doing so would be likely to prejudice those negotiations.

Refusing to Respond to a Request
The Trust can refuse to comply with a request if the request is manifestly unfounded or excessive, taking into account whether the request is repetitive in nature.

If a request is found to be manifestly unfounded or excessive the Trust can:

- request a "reasonable fee" to deal with the request; or
- refuse to deal with the request.

In either case the Trust need to justify the decision and inform the requester about the decision.

The reasonable fee should be based on the administrative costs of complying with the request. If deciding to charge a fee the Trust should contact the individual promptly and inform them. The Trust do not need to comply with the request until the fee has been received.

Record Keeping
A record of all subject access requests shall be kept by the DPO and School Business Manager. The record shall include the date the SAR was received, the name of the requester, what data the Trust sent to the requester and the date of the response.

Appendix B – Online Links and Form to Make a Subject Access Request

The Data Protection Act 2018 provides the data subject with a right to receive a copy of the data/information the Trust hold about the data subject or to authorise someone to act on the data subject's behalf. The following links should be accessed or the form below completed (for posting) i to make a request for data. The request will normally be processed within one calendar month upon receipt of a fully completed form and proof of identity.

Proof of Identity
The Trust requires proof of your identity before we can disclose personal data. Proof of your identity should include a copy of a document such as your birth certificate, passport, driving licence, official letter addressed to you at your address e.g., bank statement, recent utilities bill or council tax bill. The document should include your name, date of birth and current address. If you have changed your name, please supply relevant documents evidencing the change.

A request can be made online through the following links:

The 3-18 Education Trust

Bowbrook Primary School

Bridgnorth Endowed School

Coleham Primary School

Much Wenlock Primary School

St Martins School

The Priory School

The Thomas Adams School

William Brookes School

Hodnet Primary School

John Wilkinson Primary School

A request can be made by post to the following name and address:

Data Protection Officer for The 3-18 Education Trust
Judicium Consulting Limited
5th Floor
98 Theobalds Road
London
WC1X 8WB

Please enclose a completed request form and proof of identity.

A request can be made by email to: dataservices@judicium.com

Please attach a completed request form and proof of identity.

Subject Access Request Form

Section 1
Please fill in the details of the data subject (i.e., the person whose data you are requesting). If you are not the data subject and you are applying on behalf of someone else, please fill in the details of the data subject below and not your own.

Title	
Surname/Family Name	
First Name(s)/ Forename	
Date of Birth	
Address	
Post Code	
Phone Number	
Email address	

I am enclosing the following copies as proof of identity (please tick the relevant box):

Birth certificate
Driving licence
Passport
An official letter to my address

Personal Information If you only want to know what information is held in specific records, please indicate in the box below. Please tell us if you know in which capacity the information is being held, together with any names or dates you may have. If you do not know exact dates, please give the year(s) that you think may be relevant.
Details:

Employment records:

If you are, or have been employed by the School and are seeking personal information in relation to your employment please provide details of your staff number, unit, team, dates of employment etc.

Details:

Section 2
Please complete this section of the form with your details if you are acting on behalf of someone else (i.e., the data subject).

If you are NOT the data subject, but an agent appointed on their behalf, you will need to provide evidence of your identity as well as that of the data subject and proof of your right to act on their behalf.

Title	
Surname/ Family Name	
First Name(s)/Forenames	
Date of Birth	
Address	
Post Code	
Phone Number	

I am enclosing the following copies as proof of identity (please tick the relevant box):	
	Birth certificate
	Driving licence
	Passport
	An official letter to my address

What is your relationship to the data subject? (e.g., parent, carer, legal representative)	
I am enclosing the following copy as proof of legal authorisation to act on behalf of the data subject:	
	Letter of authority
	Lasting or Enduring Power of Attorney
	Evidence of parental responsibility
	Other (give details):

Section 3
Please describe as detailed as possible what data you request access to (e.g., time period, categories of data, information relating to a specific case, paper records, electronic records).

I wish to:	
	Receive the information by post*
	Receive the information by email

	Collect the information in person
	View a copy of the information only
	Go through the information with a member of staff
*Please be aware that if you wish us to post the information to you, we will take every care to ensure that it is addressed correctly. However, we cannot be held liable if the information is lost in the post or incorrectly delivered or opened by someone else in your household. Loss or incorrect delivery may cause you embarrassment or harm if the information is 'sensitive'.	