DDAT
Derby Diocesan Academy Trust

Diocese of Derby
THE CHURCH OF ENGLAND

Derby Diocesan Academy Trust 2

DATA PROTECTION POLICY

Date of adoption: 28th September 2021
Date to be revised: 30th September 2023

1 Policy Statement

The Data Protection Act 2018 (DPA 2018) sets out the framework for data protection law in the UK. It sits alongside the UK General Data Protection Regulation (UK GDPR) and tailors how the UK GDPR applies. The UK GDPR sets out the key principles, rights and obligations for most processing of personal data. Together, these are the rules that protect personal privacy and uphold individual's rights. These rules apply to anyone who handles or has access to people's personal data.

This policy is intended to ensure that personal information is dealt with properly and securely and in accordance with the legislation. It will apply to personal information regardless of the way it is used, recorded and stored, and applies to personal information held in both paper and electronic files.

This policy has due regard to all relevant legislation and statutory guidance including, but not limited to, the following:

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

This policy also has regard to the following guidance:

- ICO (2021) 'Guide to the UK General Data Protection Regulation (UK GDPR)'
- DfE (2018) 'Data protection: a toolkit for schools'
- ICO (2012) 'IT asset disposal for organisations'

2 Policy Objectives

DDAT2 (also known as 'the Trust'), as the Data Controller, will comply with its obligations under the UK GDPR and DPA 2018. DDAT2 is committed to being concise, clear and transparent about how it obtains and uses personal data and will ensure Data Subjects are aware of their rights under the legislation.

All staff must have a general understanding of the law and understand how it may affect their decisions in order to make an informed judgement about how information is gathered, used and ultimately deleted on our behalf. Any questions about the operation of this Policy or any concerns that the Policy has not been followed should be referred in the first instance to the Data Protection Officer (DPO). The DPO is Jason Hampton who can be contacted at ddatadmin@ddat.org.uk or on 0333 3554353.

The Information Commissioner, as the UK's independent authority, can impose fines for serious breaches of data protection legislation. It is imperative that the Trust; all schools within the Trust; and all staff and volunteers comply with the legislation and with this policy.

3 Scope of the Policy

Personal data is any information that relates to an identified or identifiable living individual who can be identified directly or indirectly from the information (UK GDPR Article 4 Definitions). The information includes factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of a living individual. This includes any expression of opinion about an individual and intentions towards an individual. Under the UK GDPR, personal information also includes an identifier such as a name, an identification number, location data or an online identifier, such as an IP address. The UK GDPR applies to both automated personal data and to manual filing systems, where personal data is accessible according to specific criteria, as well as to chronologically ordered data and pseudonymised data, e.g. key-coded.

DDAT2 and its schools collect large amounts of personal data every year about current, past and prospective staff members, pupils, their families, volunteers and external contractors, in accordance with its legal obligations under data protection legislation. This includes pupil records, staff records, names and addresses of those requesting prospectuses; examination marks; references; fee collection; as well as the many different types of research data used by the Trust. In addition, it may be required by law to collect and use certain types of information to comply with statutory obligations of Local Authorities (LAs), government agencies and other bodies.

This Policy, and other documents referred to in it, set out the basis on which the Trust will process any personal data it collects from individuals, whether that data is provided to us by individuals or obtained from other sources. It sets out the rules on data protection and the legal conditions that must be satisfied when we obtain, handle, process, transfer and store personal data. This Policy does not form part of any employee's contract of employment and may be amended at any time.

4 Data Protection Principles

Anyone processing personal data for or on behalf of the Trust must comply with the principles set out in the UK GDPR. These principles state that personal data must be:

- Processed lawfully, fairly and in a transparent manner (**lawfulness, fairness and transparency**).
- Collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes (**purpose limitation**).
- Adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed (**data minimisation**).
- Accurate and, where necessary, kept up-to-date; every reasonable step must be taken to ensure that personal data that is inaccurate is erased or rectified without delay (**accuracy**).
- Kept in a form which permits identification of Data Subjects for no longer than is necessary for the purposes for which the personal data is processed (**storage limitation**).
- Processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures (**integrity and confidentiality**).

The UK GDPR also requires that “the controller shall be responsible for, and able to demonstrate, compliance with” the above principles.

5 Transfer Limitation

In addition, personal data shall not be transferred to a country outside the United Kingdom (UK) unless that country or territory ensures an adequate level of protection for the rights and freedoms of Data Subjects in relation to the processing of personal data or where the organisation receiving the data has provided adequate safeguards (these safeguards may be provided by a legally binding agreement between public authorities or bodies, standard data protection clauses provided by the ICO or certification under an approved mechanism).

This means that individuals' rights must be enforceable and effective legal remedies for individuals must be available following the transfer. It may also be possible to transfer data where the Data Subject has provided explicit consent or for other limited reasons. Staff should contact the DPO if they require further assistance with a proposed transfer of personal data outside of the UK.

6 Lawful basis for processing Personal Data

Before any processing activity starts for the first time, and then regularly afterwards, the purpose(s) for the processing activity and the most appropriate lawful basis for that processing must be selected:

- Processing is necessary for the performance of a task carried out **in the public interest** or in the exercise of official authority vested in the Trust.
- Processing is necessary for the **performance of a contract** to which the Data Subject is party, or in order to take steps at the request of the Data Subject prior to entering into a contract.
- Processing is necessary for **compliance with a legal obligation** to which the Data Controller is subject.
- Processing is necessary in order to protect the **vital interests** of the Data Subject or of another natural person.
- Processing is necessary for the purposes of the **legitimate interests** pursued by the Data Controller or by a third party (this condition is not available to processing undertaken by the Trust in the performance of its tasks).
- The Data Subject has given **consent** (see section 7 below) to the processing of his or her data for one or more specific purposes.

Where a significant privacy impact is identified, a data protection impact assessment (DPIA) may also need to be conducted (see section 11).

7 Consent

Consent must be a positive indication expressly confirmed in words. It cannot be inferred from silence, inactivity, a positive action without words or pre-ticked boxes. Consent will only be accepted where it is freely given, specific, informed and an unambiguous indication of the individual's wishes. Consent can be withdrawn by the individual at any time. Where consent is given, a record will be kept documenting how and when consent was given, and what the data subject was told.

The Trust ensures that consent mechanisms meet the standards of the UK GDPR. Where the standard of consent cannot be met, an alternative legal basis for processing the data must be found, or the processing must cease. Consent accepted under the DPA 2018 will be reviewed to ensure it meets the standards of the UK GDPR; however, acceptable consent obtained under the DPA 2018 will not be reobtained. Consent may need to be refreshed if personal

data is intended to be processed for a different and incompatible purpose which was not disclosed when the Data Subject first gave consent.

When pupils and staff join the school, the staff member or pupil (or, where appropriate, pupil's parent) will be required to complete a consent form for personal data use. This consent form deals with the taking and use of photographs and videos, amongst other things. Where appropriate, third parties may also be required to compete a consent form.

Parental consent to data processing must be obtained for pupils or other children younger than 13 years of age. A young person aged 13 or over is able to give or revoke consent (unless they do not have capacity). Where consent is required from a young person aged 13 or over the requirements in relation to consent, as set out for adults, still apply and the information in relation to such consent must be made clear to the young person.

8 Safeguarding

The UK GDPR does not prevent, or limit, the sharing of information for the purposes of keeping children safe, and information may be shared without consent if to gain consent would place a child at risk.

The Trust understands that the UK GDPR does not prevent or limit the sharing of information for the purposes of keeping children safe. The Trust will ensure that information pertinent to identify, assess and respond to risks or concerns about the safety of a child is shared with the relevant individuals or agencies proactively and as soon as is reasonably possible. Where there is doubt over whether safeguarding information is to be shared, especially with other agencies, the Designated Safeguarding Lead (DSL) will ensure that they record the following information:

- Whether data was shared
- What data was shared
- With whom data was shared
- For what reason data was shared
- Where a decision has been made not to seek consent from the data subject or their parent
- The reason that consent has not been sought, where appropriate

The Trust will aim to gain consent to share information where appropriate however the Trust will not endeavour to gain consent if to do so would place a child at risk. The Trust will manage all instances of data sharing for the purposes of keeping a child safe in line with the Trust's Safeguarding Policy.

9 Sensitive Personal Information

Sensitive personal information ('Special Categories of Personal Data') is data which reveals racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, sex life or orientation or is genetic or biometric data which uniquely identifies a natural person. Sensitive personal information will only be processed if there is a lawful basis for doing so, as identified in section 6, and under the following conditions:

- The Data Subject has given explicit consent (which has been clearly explained in a Privacy Notice)
- Processing is carried out by a not-for-profit body with a political, philosophical, religious or trade union aim provided the processing relates only to members or former members

(or those who have regular contact with it in connection with those purposes) and provided there is no disclosure to a third party without consent

- Processing relates to personal data manifestly made public by the data subject
- Processing is necessary for:
  - Carrying out obligations under employment, social security or social protection law, or a collective agreement
  - Protecting the vital interests of a data subject or another individual where the data subject is physically or legally incapable of giving consent
  - The establishment, exercise or defence of legal claims or where courts are acting in their judicial capacity
  - Reasons of substantial public interest with a basis in law which is proportionate to the aim pursued and which contains appropriate safeguards including the safeguarding of children and individuals at risk (see section 8); the prevention of fraud; and preventing or detecting unlawful acts
  - The purposes of preventative or occupational medicine, for assessing the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment or management of health or social care systems and services with a basis in law
  - Reasons of public interest in the area of public health, such as protecting against serious cross-border threats to health or ensuring high standards of healthcare and of medicinal products or medical devices
  - Archiving purposes in the public interest, or scientific and historical research purposes or statistical purposes in accordance with a basis in law

When none of the above apply, consent will be obtained by the data subject to the processing of their special category personal data. The Trust's Privacy Notices set out the types of sensitive personal information that it processes, what it is used for, the lawful basis for the processing and the special condition that applies. Please refer to the Trust's website (https://ddat.org.uk/gdpr).

Sensitive personal information will not be processed until an assessment has been made of the proposed processing as to whether it complies with the criteria above and the individual has been informed (by way of a Privacy Notice or consent) of the nature of the processing, the purposes for which it is being carried out, the legal basis for it and the right of the data subject to raise a complaint with the ICO in relation to any processing.

There may be circumstances where it is considered necessary to process personal data or special category personal data in order to protect the vital interests of a data subject. This may include medical emergencies where it is not possible for the data subject to give consent to the processing.

Where the Trust relies on:

- 'Performance of contract' to process a child's data, the Trust considers the child's competence to understand what they are agreeing to, and to enter into a contract.
- 'Legitimate interests' to process a child's data, the Trust takes responsibility for identifying the risks and consequences of the processing and puts age-appropriate safeguards in place.
- Consent to process a child's data, the Trust ensures that the requirements outlined in section 7 are met, and the school does not exploit any imbalance of power in the relationship between the school and the child.

'Sensitive personal data' does not include data about criminal allegations, proceedings or convictions. In the case of criminal offence data, the Trust is only able to process this if it is either under the control of official authority or authorised by domestic law. The latter point can only be used if the reason for storing and requiring the data meets one of the conditions below:

- The processing is necessary for the purposes of performing or exercising obligations or rights which are imposed or conferred by law on the controller of the data subject in connection with employment, social security, social protection, health or social care purposes, public health and research.

10 Automated Decision Making

Where the Trust or its schools carry out automated decision making it must meet all the principles and have a lawful basis for the processing. The Trust must, as soon as reasonably possible, notify the Data Subject in writing that a decision has been taken based on solely automated processing and that the Data Subject may request the Trust to reconsider or take a new decision. If such a request is received staff must contact the DPO.

Automated decisions will not concern a child nor use special category personal data unless the Trust has the explicit consent of the individual or the processing is necessary for reasons of substantial public interest.

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

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

11 Data Protection Impact Assessments (DPIA)

All data controllers are required to implement 'Privacy by Design' when processing personal data. This means that the processes used by the Trust and its schools must embed privacy considerations and incorporate appropriate technical and organisational measures (like pseudonymisation) in an effective manner to ensure compliance with data privacy principles.

Where processing is likely to result in high risk to an individual's data protection rights (for example where a new technology is being implemented) a DPIA must be carried out to assess:

- Whether the processing is necessary and proportionate in relation to its purpose.
- The risks to individuals.
- What measures can be put in place to address those risks and protect personal information.

Staff should adhere to the Data Protection Toolkit for Schools from the DfE with reference to the DPIA template. When carrying out a DPIA, staff should seek the advice of the DPO for support and guidance and once complete, refer the finalised document to the DPO for sign off.

12 Documentation and records

Written record of processing activities must be kept and recorded including:

- The name(s) and details of individuals or roles that carry out the processing.
- The purposes of the processing.
- A description of the categories of individuals and categories of personal data.
- Categories of recipients of personal data.
- Details of transfers to third countries, including documentation of the transfer mechanism safeguards in place.
- Retention schedules.
- A description of technical and organisational security measures.

It is the responsibility of all staff to ensure that the register of processing activities is accurate and kept up to date. The School Business Manager (SBM) must enter details of the school's suppliers into the GDPRiS system either directly or with the assistance of the DPO.

13 Privacy Notices

The Trust and its schools will issue Privacy Notices as required, informing Data Subjects (or their parents, depending on age of the pupil, if about pupil information) about the personal information that is collected and held in relation to individual Data Subjects, how individuals can expect their personal information to be used and for what purposes.

When information is collected directly from Data Subjects, including for HR or employment purposes, the Data Subject shall be given all the information required by the UK GDPR, including the identity of the Data Controller and the DPO; and how and why the Trust and its schools will use, process, disclose, protect and retain that personal data through a Privacy Notice (which must be presented when the Data Subject first provides the data).

When information is collected indirectly (for example from a third party or publicly available source) the Data Subject must be provided with all the information required by the UK GDPR as soon as possible after collecting or receiving the data. The Trust and its schools must also check that the data was collected by the third party in accordance with the UK GDPR and on a basis which is consistent with the proposed processing of the personal data. Privacy Notices will be in writing or via a link from the School's website to the Trust's website (https://ddat.org.uk/gdpr) unless the individual requests an oral notification.

14 Purpose Limitation

Personal data must be collected only for specified explicit and legitimate purposes. It must not be further processed in any manner incompatible with those purposes. Personal data must not be used for new, different or incompatible purposes from that disclosed when it was first obtained unless the Data Subject has been informed of the new purposes and they have consented where necessary.

15 Data minimisation and retention

Personal data must be adequate, relevant and limited to what is necessary in relation to the purposes for which it is processed. Staff may only process data when their role requires it. Staff must not process personal data for any reason unrelated to their role.

The Trust maintains a Retention Schedule based on guidance from the Information Records Management Society (IRMS Schools Toolkit) to ensure personal data is deleted after a

reasonable time after the purpose for which it was being held unless a law requires the data to be kept for a minimum time. Staff must take all reasonable steps to destroy or delete all personal data that is held in its systems when it is no longer required in accordance with the Schedule. This includes requiring third parties to delete data where applicable.

If a member of staff has any doubt as to whether any personal data has been or will be kept longer than is necessary for the purpose or purposes for which they were collected or has any doubt as to whether any processing exceeds the purposes for which that data was originally collected, he or she should notify the Data Protection Officer.

16 Individual Rights

We are committed to upholding the rights of individuals to access personal data the Trust and its schools hold on them. Individuals have the following rights in relation to their personal information:

- To be informed about how, why and on what basis that information is processed (see the relevant Privacy Notice available at https://ddat.org.uk/gdpr on the Trust's website).
- To obtain confirmation that personal information is being processed and to obtain access to it and certain other information, by making a Subject Access Request (SAR). Please refer to Appendix 1 – 'Procedure for Access to Personal Information'.
- To have data corrected if it is inaccurate or incomplete (see section 17, 'Accuracy').
- To have data erased if it is no longer necessary for the purpose for which it was originally collected or processed, or if there are no overriding legitimate grounds for the processing ('the right to be forgotten').
- To restrict the processing of personal information where the accuracy of the information is contested, or the processing is unlawful (but the individuals does not want the data to be erased) or where the Trust no longer needs the personal information, but the data is required to establish, exercise or defend a legal claim.
- To restrict the processing of personal information temporarily where you do not think it is accurate (and the Trust is verifying whether it is accurate), or where you have objected to the processing (and the Trust is considering whether its legitimate grounds override your interests).
- In limited circumstances to receive or ask for their personal data to be transferred to a third party in a structured, commonly used and machine-readable format.
- To withdraw consent to processing at any time (if applicable).
- To request a copy of an agreement under which personal data is transferred outside of the UK.
- To object to decisions based solely on automated processing, including profiling.
- To be notified of a data breach which is likely to result in high risk to their rights and obligations.
- To make a complaint to the ICO or a Court.

17 Accuracy

It is the responsibility of staff to ensure that personal data is accurate at the point of collection and kept up to date at regular intervals afterwards. Parents and anyone who provides personal data should also inform the Trust as soon as possible if there is any change to their personal data.

The Trust will take all reasonable steps to destroy or amend inaccurate or out-of-date data and will implement a proportional response for data that has a significant impact on the individual, e.g. if significant decisions are made using that data. The school will restrict processing of the data in question whilst its accuracy is being verified, where possible.

Requests for rectification will be responded to within one month; this will be extended by two months where the request for rectification is complex. Requests will be investigated and resolved, where appropriate, free of charge; however, the Trust may impose a 'reasonable fee' to cover the administrative costs of complying with requests that are manifestly unfounded or excessive or if an individual makes multiple requests at once. The Trust may refuse to process requests for rectification if they are manifestly unfounded or excessive or if exemptions apply.

18 Individual Responsibilities

During their employment, staff may have access to the personal information of other members of staff, suppliers, clients or the public. The Trust expects staff to help meet its data protection obligations to those individuals. All staff must complete the mandatory online data protection training.

If you have access to personal information, you must:

- Only access the personal information that you have authority to access and only for authorised purposes.
- Only allow other staff to access personal information if they have appropriate authorisation.
- Only allow individuals who are not Trust staff to access personal information if you have specific authority to do so.
- Keep personal information secure (e.g. by complying with rules on access to premises, computer access, password protection and secure file storage and destruction in accordance with the Trust's policies).
- Not remove personal information, or devices containing personal information (or which can be used to access it) from the Trust's premises unless appropriate security measures are in place (such as pseudonymisation, encryption or password protection) to secure the information and the device.
- Not store personal information on local drives or on personal devices that are used for work purposes.

19 Information security

The Trust and it schools will use appropriate technical and organisational measures to keep personal data secure, to protect against unauthorised or unlawful processing and against accidental loss, destruction or damage. All staff are responsible for keeping information secure in accordance with the legislation and must follow the Trust's acceptable usage policy.

The Trust will develop, implement and maintain safeguards appropriate to its size, scope and business, its available resources, the amount of personal data that it owns or maintains on behalf of others and identified risks (including use of encryption and pseudonymisation where applicable). It will regularly evaluate and test the effectiveness of those safeguards to ensure security of processing.

Staff must guard against unlawful or unauthorised processing of personal data and against the accidental loss of, or damage to, personal data. Staff must exercise particular care in

protecting sensitive personal data from loss and unauthorised access, use or disclosure. Staff must notify their line manager, the Headteacher or the DPO immediately of any personal data breaches, allegations of personal data breaches or suspicions of personal data breaches

Staff must follow all procedures and technologies put in place to maintain the security of all personal data from the point of collection to the point of destruction. Staff may only transfer personal data to third-party service providers who agree in writing to comply with the required policies and procedures and who agree to put adequate measures in place, as requested.

Staff must maintain data security by protecting the **confidentiality, integrity and availability** of the personal data, defined as follows:

- **Confidentiality** means that only people who are authorised to use the personal data can access it.
- **Integrity** means that personal data is accurate and suitable for the purpose for which it is processed.
- **Availability** means that authorised users can access personal data when they need it for authorised purposes.

Security procedures include:

- **Entry controls**: any stranger seen in entry-controlled areas should be reported.
- **Secure lockable desks and cupboards**: desks and cupboards should be kept locked if they hold confidential information of any kind (personal information is always considered confidential).
- **Methods of disposal**: paper documents should be shredded. Digital storage devices should be professionally processed and physically destroyed when they are no longer required.
- **Equipment**: Staff must ensure that individual monitors do not show confidential information to passers-by and that they log off from or password protect their computers, tablets or other devices when left unattended.
- **Data storage methods**: measures to store data securely, such as Pseudonymisation or key-coding, must be implemented where appropriate.

Where possible, staff, governors and trustees will not use their personal laptops or computers for school purposes. All necessary members of staff are provided with their own secure login and password, and every computer regularly prompts users to change their password. Where personal information that could be considered private or confidential is taken off the premises, either in electronic or paper format, staff will take extra care to follow the same procedures for security, e.g. keeping devices under lock and key. The person taking the information from the school premises accepts full responsibility for the security of the data.

Staff must comply with and not attempt to circumvent the administrative, physical and technical safeguards the Trust has implemented and maintains in accordance with the UK GDPR and DPA 2018.

Where the Trust and its schools use external organisations to process personal information on its behalf, additional security arrangements need to be implemented in contracts with those organisations to safeguard the security of personal information. Contracts with external organisations must provide that:

- The organisation may only act on the written instructions of the Trust or its schools.
- Those processing data are subject to the duty of confidence.

- Appropriate measures are taken to ensure the security of processing.
- Sub-contractors are only engaged with the prior consent of the Trust and under a written contract.
- The organisation will assist the Trust in providing subject access and allowing individuals to exercise their rights in relation to data protection.
- The organisation will delete or return all personal information to the Trust or the school as requested at the end of the contract.
- The organisation will submit to audits and inspections, provide the Trust with whatever information it needs to ensure that they are both meeting their data protection obligations, and tell the Trust immediately if it does something infringing data protection law.

Before any new agreement involving the processing of personal information by an external organisation is entered into, or an existing agreement is altered, the relevant staff must seek approval from the DPO.

20 Data breaches

The term 'personal data breach' refers to a breach of security which has led to the destruction, loss, alteration, unauthorised disclosure of, or access to, personal data. The headteacher will ensure that all staff members are made aware of, and understand, what constitutes a data breach as part of their training. A data breach may take many different forms:

- Loss or theft of data or equipment on which personal information is stored.
- Unauthorised access to or use of personal information either by a member of staff or third party.
- Loss of data resulting from an equipment or systems (including hardware or software) failure.
- Human error, such as accidental deletion or alteration of data.
- Unforeseen circumstances, such as a fire or flood.
- Deliberate attacks on IT systems, such as hacking, viruses or phishing scams.
- Blagging offences where information is obtained by deceiving the organisation which holds it.

Where the school faces a data security incident, the DPO will coordinate an effort to establish whether a personal data breach has occurred, assess the significance of any breach, and take prompt and appropriate steps to address it.

In the event of a suspected data breach, staff should follow the procedure set out in Appendix 2. Staff must ensure they inform their line manager or the School Business Manager (SBM) immediately and make all reasonable efforts to recover the information. The line manager, SBM or Headteacher must inform the DPO. In the event the line manager, SBM or Headteacher is unavailable, staff should inform the DPO directly.

The DPO will notify the Information Commissioner's Office, where necessary, in respect of any relevant breach without undue delay. If any personal data breach is likely to adversely affect individual's rights and freedoms, the Trust will inform those individuals without undue delay.

21 Training

Schools will ensure that all staff and volunteers are adequately trained regarding their data protection responsibilities. As a minimum, all staff and volunteers must complete the online data protection training available to schools from the DPO and via the GDPRiS system on an annual basis. Schools should contact the DPO for further collateral or additional onsite support, as required.

22 Consequences of a failure to comply

Any failure to comply with any part of this policy may lead to disciplinary action under the Trust's procedures and this action may result in dismissal for gross misconduct. If a non-employee breaches this policy, they may have their contract terminated with immediate effect.

If you have any questions or concerns about this policy, you should contact your line manager or the Trust's DPO.

23 Policy Review

This policy will be updated as necessary to reflect best practice or amendments made to the UK GDPR or DPA 2018.

24 The Supervisory Authority in the UK

Please follow this link to the ICO's website (https://ico.org.uk/) which provides detailed guidance on a range of topics including individuals' rights, data breaches, dealing with subject access requests and how to handle requests from third parties for personal data.

25 Glossary

In this Policy, the functions of the Trust are the provision of education and any pastoral, business, administrative, community or similar activities associated with that provision. References to the Trust 'carrying out its functions' or similar are references to these activities.

Automated Decision-Making (ADM) is when a decision is made which is based solely on automated processing (including profiling) which produces legal effects or significantly affects an individual. The UK GDPR prohibits automated decision-making (unless certain conditions are met) but not automated processing.

Automated Processing is 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. Profiling is an example of automated processing.

Consent is agreement which must be freely given, specific, informed and be an unambiguous indication of the Data Subject's wishes by which they, by a statement or by a clear positive action, which signifies agreement to the processing of personal data relating to them.

Criminal Convictions and Offences means the commission of, or proceedings for, any offence committed or alleged to have been committed by a person, the disposal of such proceedings or the sentence of any court in such proceedings.

Data Subjects means identified or identifiable natural persons whose personal data the Trust holds. This Policy also refers to Data Subjects as '**individuals**'.

Data Controllers are the people who, or organisations which, determine the purposes for which any personal data is processed, including the means of the processing. The Trust is the Data Controller of all personal data used for carrying out its functions.

Data Protection Officer (DPO) is the person required to be appointed in public authorities under the UK GDPR.

Data Users are, for the purposes of this Policy, those of our employees whose work involves processing personal data. Data Users must protect the data they handle in accordance with this Policy and any applicable data security procedures at all times. This Policy also refers to Data Users as '**Trust staff**' or simply '**staff**'.

Data Processors include any person or organisation, who is not a member of Trust staff, which processes personal data on our behalf. Employees of Data Controllers are excluded from this definition, but it could include suppliers that handle personal data on the Trust's behalf.

Fair Processing Notices are documents explaining to Data Subjects how their data will be used by the Trust. This Policy also refers to Fair Processing Notices as '**Privacy Notices**'.

Personal Data means any information relating to an identified or identifiable natural person; an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

Personal Data Breach means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed.

Pseudonymisation means the processing of personal data so that it can no longer be attributed to a specific person without the use of additional information, provided that such additional information is kept separately and is subject to measures to ensure that the personal data is not attributed to an identified or identifiable natural person.

Relevant Data Protection Law means the UK General Data Protection Regulation, the Data Protection Act 2018 and any successor legislation, the Privacy and Electronic Communications (EC Directive) Regulations 2003 (SI 2003/2426) and all applicable laws and regulations relating to the processing of personal data and privacy as amended, re-enacted, replaced or superseded from time to time and where applicable the guidance and codes of practice issued by the United Kingdom's Information Commissioner.

Special Categories of Personal Data (formerly known as '**Sensitive Personal Data**') include information about a person's racial or ethnic origin, political opinions, religious or similar beliefs, trade union membership, physical or mental health or condition, sexual life and genetic or biological traits. Special Categories of personal data can only be processed under strict conditions.

26 Appendix 1: Procedure for Access to Personal Data

26.1 Right of access to information

There are two distinct rights of access to personal data held by educational establishments:

- **Under the UK GDPR and the Data Protection Act 2018** (the 'DPA 2018') an individual has a right to request access to their own personal information. In certain circumstances requests may be made by a parent on behalf of their child.
- **The Education (Pupil Information) (England) Regulations 2005** (the 'Regulations') gives parents the right of access to their child's curricular and educational records in a maintained school.

  There is not an equivalent legal right of access to information if the child attends an Academy, Independent or Free School.

26.2 DPA 2018: The subject access right

Under the DPA 2018, individuals, including a pupil or someone acting on their behalf, has the right to obtain confirmation that their data is being processed and to obtain a copy of their personal data, as well as other supplementary information, in order to verify the lawfulness of the processing. An individual is only entitled to their own personal data, and not to information relating to other people (unless the information is also about them, or they are acting on behalf of someone).

In addition to a copy of their personal data, individuals have to be provided with the following information, much of which is already included in the Trust's Privacy Notice:

- The purposes for processing their data;
- The categories of personal data concerned;
- The recipients or categories of recipient the Trust discloses the personal data to;
- The retention period for storing the personal data or, where this is not possible, the criteria for determining how long you will store it;
- The existence of their right to request rectification, erasure or restriction or to object to such processing;
- The right to lodge a complaint with the ICO or another supervisory authority;
- Information about the source of the data, where it was not obtained directly from the individual;
- The existence of automated decision-making (including profiling); and
- The safeguards provided if the Trust transfers personal data to a third country or international organisation.

<u>How should a request be made?</u>

The Trust asks that individuals who wish to make a request write to the Headteacher or use the enclosed form (see Appendix 3) to help the Trust locate the information they want. From a legislative point of view, the UK GDPR does not specify how to make a valid request. Therefore, an individual could make a Subject Access Request (SAR) verbally or in writing. It can also be made to any part of the Trust (including by social media) and does not have to be to a specific person or contact point.

The Trust will verify the identity of the person making the request before any information is supplied. If necessary, proof of identify may be requested, however the Trust will only ask for information that is necessary to confirm the individual's identity.

Children have the same rights of access to their own personal information as adults, and the same rights of privacy. There is no minimum age in English law, however current practice accepts that, provided a child is mature enough to understand their rights, a child of, or over the age of 13 years shall be considered capable of giving consent. This does not rule out receipt of a valid request from a child of a younger age, as each request should be considered on its merits on an individual basis.

When a SAR is received from a child, it will need to be judged whether the child has the capacity to understand the implications of their request and of the information provided as a result of that request. If the child does understand then their request will be dealt with in the same way as that of an adult.

Response time

All requests will be responded to without delay and, at the latest, within one month following date of receipt. The timeframe may be extended by a further two months but only where requests are complex or numerous. If this is the case, the individual must be informed within one month of the receipt of the request and it must be explained why the extension is necessary.

If additional information has been requested from the individual, such as proof of identity, then the period for responding to the request begins when the Trust receives the additional information.

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

Charges

A copy of the information will be supplied to the individual free of charge; however, the Trust may impose a 'reasonable fee' to comply with requests for further copies of the same information. All fees will be based on the administrative cost of providing the information.

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

Exemptions

There are some exemptions to the right to subject access that apply in certain circumstances or to certain types of personal information. This means all information must be reviewed prior to disclosure. Included below are some of the exemptions that apply to a Trust, this is not an exhaustive list.

Third Party information: If the information held identifies other people, then it will sometimes be right to remove or edit that information so as not to reveal the identity of the third parties, unless the third parties have agreed to the disclosure. This is less likely to apply to information identifying teachers or other professionals unless to disclose it would cause them serious harm.

Reasonable steps must be taken to obtain third party consent to disclosure. If the third parties cannot be located or do not respond it may still be reasonable to consider disclosure if the information is of importance to the Data Subject. The Trust must still adhere to the one month statutory timescale.

Where redaction has taken place then a full copy of the information provided should be retained in order to establish, if a complaint is made, what was redacted and why.

Information disclosed should be clear, meaning any codes or technical terms will need to be clarified and explained. If information contained within the disclosure is difficult to read or illegible, then it should be retyped. However, the Trust is not required to ensure that the information is provided in a form that can be understood by the particular individual making the request.

Information likely to cause serious harm or distress: Any information which may cause serious harm to the physical or mental health or emotional condition of the pupil or another individual involved should not be disclosed, nor should information that would reveal that the child is at risk of abuse, or information relating to court proceedings.

Crime and Disorder: If the disclosure of the information is likely to hinder the prevention or detection of a crime, the prosecution or apprehension of offenders, or the assessment or collection of any tax or duty, the information should be withheld.

Legal professional privilege: If the information is general legal advice or advice which relates to anticipated or pending legal proceedings it is subject to 'legal professional privilege'. The disclosure of any communication to or from a legal advisor to another person (including the Data Subject) should not take place unless this has first been discussed with the legal advisor concerned.

References: The right of access does not apply to references given, or to be given, in confidence.

Absence of or invalid consent to disclosure: If the Data Subject is considered incapable of giving valid consent to disclosure (i.e. they do not have the capacity to understand the nature/implications of the access request), or if it is suspected that the consent was obtained under duress by someone acting on their behalf, or based on misleading information, then access should be refused.

26.3 The Education Regulations: Parents' right of access

DDAT2 is a multi-academy trust (MAT) and, as such, there is no legal right of access under the Education (Pupil Information) (England) Regulations 2005 to a child's educational record.

26.4 Complaints

Complaints about the above procedures should be made to the Data Protection Officer (DPO) who will decide whether it is appropriate for the complaint to be dealt with in accordance with the Trust's complaint procedure.

Complaints which are not appropriate to be dealt with through the Trust's complaint procedure can be dealt with by the Information Commissioner. Contact details of both will be provided with the disclosure information.

26.5 Contact

If you have any queries or concerns regarding individuals right of access to their own personal information, please contact:

Jason Hampton,
Data Protection Officer,
Deepdale Business Park
Ashford Road
Bakewell
DE45 1GT

Email: ddatadmin@ddat.org.uk
DDAT2 ICO registration number: ZA129135

Further advice and information can be obtained from the Information Commissioner's Office at www.ico.gov.uk.

27 Appendix 2: Personal data breach procedure

This procedure is based on guidance on personal data breaches produced by the ICO.

- On finding or causing a breach, or potential breach, the staff member or Data Processor must immediately notify their line manager, the Headteacher or DPO (ddatadmin@ddat.org.uk).
- The DPO will investigate the report and determine whether a breach has occurred. To decide, the DPO will consider whether personal data has been accidentally or unlawfully:
  - Lost
  - Stolen
  - Destroyed
  - Altered
  - Disclosed or made available where it should not have been
  - Made available to unauthorised people
- The DPO will make all reasonable efforts to contain and minimise the impact of the breach, assisted by relevant staff members or data processors where necessary. (actions relevant to specific data types are set out at the end of this procedure).
- The DPO will assess the potential consequences, based on how serious they are, and how likely they are to happen.
- The DPO will work out whether the breach must be reported to the ICO. This must be judged on a case-by-case basis. To decide, the DPO will consider whether the breach is likely to negatively affect people's rights and freedoms, and cause them any physical, material or non-material damage (e.g. emotional distress), including through:
  - Loss of control over their data
  - Discrimination
  - Identify theft or fraud
  - Financial loss
  - Unauthorised reversal of pseudonymisation (for example, key-coding)
  - Damage to reputation
  - Loss of confidentiality
  - Any other significant economic or social disadvantage to the individual(s) concerned.

  If it is likely that there will be a risk to people's rights and freedoms, the DPO must notify the ICO.
- The DPO will document the decision (either way) in case that decision is challenged at a later date by the ICO or an individual affected by the breach.

- Where the ICO must be notified, the DPO will do this via the 'report a breach' page of the ICO website or by calling the ICO directly within 72 hours. As required, the DPO will set out:
    - A description of the nature of the personal data breach including, where possible:
        - The categories and approximate number of individuals concerned
        - The categories and approximate number of personal data records concerned.
    - The name and contact details of the DPO.
    - A description of the likely consequences of the personal data breach.
    - A description of the measures that have been, or will be taken, to deal with the breach and mitigate any possible adverse effects on the individual(s) concerned.
- If all the above details are not yet known, the DPO will report as much as they can within 72 hours. The report will explain that there is a delay, the reasons why, and when the DPO expects to have further information. The DPO will submit the remaining information as soon as possible.
- The DPO will also assess the risk to individuals, again based on the severity and likelihood of potential or actual impact. If the risk is high, the DPO will work with the Trust to promptly inform, in writing, all individuals whose personal data has been breached. This notification will set out:
    - The name and contact details of the DPO and relevant Trust contacts.
    - A description of the likely consequences of the personal data breach.
    - A description of the measures that have been, or will be, taken to deal with the data breach and mitigate any possible adverse effects on the individual(s) concerned.
- The DPO will notify any relevant third parties who can help mitigate the loss to individuals – for example, the police, insurers, banks or credit card companies.
- The DPO will document each breach, irrespective of whether it is reported to the ICO. For each breach, this record will include the:
    - Facts and cause
    - Effects
    - Action taken to contain it and ensure it does not happen again (such as establishing more robust processes or providing further training for individuals).

Records of all breaches will be stored within the Data Breach Log, held by the DPO and within the Trust's online system, GDPRiS. The DPO, a member of the DDAT2 central team and Headteacher will review what happened and how it can be stopped from happening again. This discussion will happen as soon as reasonably possible.

28 Appendix 3: Subject Access Request Form

To: The Head Teacher/(other – please indicate)_____

Date: _____

Dear _____,

Re: Subject Access Request

Please provide me with the information about me / my child (please delete as appropriate) that I am entitled to under the UK General Data Protection Regulation and the Data Protection Act 2018. This is so I can be aware of the information you are processing about me and verify the lawfulness of the processing.

Here is the necessary information:

My Name: _____

Relationship with the Trust. Please select:

Pupil / parent / employee / governor / volunteer / Other (please specify): _____

Correspondence address: _____

_____

_____

Contact number: _____

Email address: _____

Details of the information requested

Insert details of the information you want that will help us to locate the specific information. Please be as precise as possible, for example:

- Your personnel file
- Your child's behaviour record, held by [insert class teacher]
- Emails between 'A' and 'B' between [date]

Please provide me with:

If you need any more information from me, please let me know as soon as possible. Please bear in mind that under the UK GDPR and the Data Protection Act 2018 you cannot charge a fee to provide this information, and in most cases, must supply me with the information within 1 month.

If you need any advice on dealing with this request, you can contact the Information Commissioner's Office on 0303 123 1113 or at www.ico.org.uk

Yours sincerely,