Data Protection Policy

Responsibility for Review: Chief Executive, Dixons Academies Trust
Date of Last Review: February 2024

Policy document provenance

Approver:	Trust Board
Date of approval:	8 February 2024
Policy owner:	Chief executive
Policy authors	Head of governance
Date of next review:	January 2026
Summary of changes in this review	• All references to GDPR now refer to the UK GDPR • Local governing bodies have changed to local academy boards • Updated data protection impact assessment process • Updated data breach reporting process • Updated subject access request guidance
Related policies and documents:	• Protection of biometric information policy • Online safety policy and acceptable use policy • Data breach management procedure • Data classification, handling and disposal policy • Records and retention policy • Data governance policy • Business continuity policies • Data protection impact assessments (DPIA) workbook and WTD • Subject access request procedure • Freedom of information policy • CCTV policy • E-security policy • Privacy notices

Unless there are legislative or regulatory changes in the interim, this policy will be reviewed on an annual basis. Should no substantive change be required at this point, the policy will move to the next review cycle.

Contents

1.0 Policy statement

Dixons Academies Trust (DAT) is required to keep and process certain information about its staff members and students in accordance with its legal obligations under the UK's General Data Protection Regulation (UK GDPR).

Our trust may, from time to time, be required to share personal information about its staff or pupils with other organisations, mainly the local authority, other academies and educational bodies, and potentially children's services.

This policy is in place to ensure that all staff and trustees are aware of their responsibilities and outlines how our trust complies with the core principles of the UK GDPR. All employees and volunteers of our trust must be made aware of our policy and procedures and must provide written acknowledgement of their understanding of their individual responsibilities in relation to the UK GDPR.

All data held by DAT business services and its academies are the responsibility of our trust.

Organisational methods for keeping data secure are imperative, and we believe that it is good practice to keep clear practical policies, backed up by written procedures.

2.0 Legal framework

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

- The UK General Data Protection Regulation
- The Data Protection Act 1998
- The Freedom of Information Act 2000
- The Education (Pupil Information) (England) Regulations 2005 (as amended in 2016)
- The Freedom of Information and Data Protection (Appropriate Limit and Fees) Regulations 2004
- School Standards and Framework Act 1998

2.2 This policy also has regard to the following guidance:

- ICO (2018) 'Guide to the General Data Protection Regulation (GDPR)'

2.3 This policy will be implemented in conjunction with the following other trust policies as listed in the provenance document.

3.0 Controller and processor

3.1 Our trust (including all academies) is both a **"Controller"** and **"Processor"** of personal data. Our trust is registered as a "Controller" with the Information Commissioner's Office.

- A **"Controller"** determines the purpose and means of processing personal data.
- A data **"Processor"** processes personal data on behalf of the data controller.

4.0 Applicable data

4.1 For the purpose of this policy, **personal data** refers to information that relates to an identifiable, living individual, e.g. employee, candidate, student, parent / carer, volunteer, contractor, freelancer, trustee, member and local academy board ambassador. The UK GDPR applies to both automated personal data and to manual filing systems, where personal data is accessible according to specific criteria:

- **Personal data** includes information such as name; address; DOB; NI Number; email address (personal and business); chronologically ordered data and pseudonymised data, e.g. UPN numbers, admission numbers, employee numbers, key-coded data; and online identifiers, e.g. IP addresses.
- **Sensitive personal data** is referred to in the UK GDPR as **'special categories of personal data',** which are broadly the same as those in the Data Protection Act (DPA) 1998. These specifically include the processing of racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, genetic data, biometric data, health, sex life and sexual orientation. In schools, this could also be staff sickness absence, diversity monitoring, photos etc. **There are strict rules surrounding the processing of special categories of personal data.**

5.0 Principles

5.1 In accordance with the requirements outlined in the GDPR, personal data will be: processed lawfully, fairly, and in a transparent manner in relation to individuals collected for specified, explicit, and legitimate purposes and not further processed in a manner that is incompatible with those purposes. Further processing for archiving purposes in the public interest, scientific or historical research purposes, or statistical purposes shall not be considered to be incompatible with the initial purposes. Adequate, relevant, and limited to what is necessary in relation to the purposes for which they are processed accurate and, when necessary, kept up to date; every reasonable step must be taken to ensure that personal data that is inaccurate, having regard to the purposes for which they are processed, is erased or rectified without delay. It must be kept in a form that permits identification of data subjects for no longer than is necessary for the purposes for which the personal data is processed; personal data may be stored for longer periods, insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes, or statistical purposes, subject to implementation of the appropriate technical and organisational measures required by the GDPR in order to safeguard the rights and freedoms of individuals. It must be 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

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

6.0 Accountability

6.1 As a publicly funded organisation, we have to appoint a **data protection officer (DPO)** and this role is carried out by the head of governance. Duties will include:

- informing and advising our trust and employees about their obligations to comply with the UK GDPR and other data protection laws
- monitoring our trust and our academies' compliance with the GDPR and other laws, including conducting internal audits, and ensuringour trust and our employees receive appropriate training and data protection awareness communications

7.0 Lawful processing

7.1 Under the UK GDPR, data will be lawfully processed under the following conditions:

- **Legal obligation**: The performance of a task for statutory / legal reasons.
- **Public interest:** The performance of a task carried out in the public interest or in the exercise of official authority vested in the controller.
- **Contractual obligation**: For the performance of a contract with the data subject or to take steps to enter into a contract, e.g. staff contracts.
- **Vital interest**: Protecting the vital interests of a data subject or another person, e.g. emergency medical situation.
- **Legitimate interest**: For the purposes of legitimate interests pursued by the controller or a third party, except where such interests are overridden by the interests, rights or freedoms of the data subject. (This condition is not available to processing undertaken by the school in the performance of its tasks.)
- **Consent**: Where processing cannot be categorised under the above conditions, the consent of the data subject must be held or obtained, e.g. sharing photographs, news stories and individual examination results.

8.0 Consent

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

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

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

8.4 Our trust ensures that consent mechanisms meet the standards of the UK GDPR. When the standard of consent cannot be met, an alternative legal basis for processing the data must be found, or the processing must cease.

8.5 Consent accepted under the Data Protection Act will be reviewed to ensure it meets the standards of the UK GDPR; however, acceptable consent obtained under the DPA will not be re-obtained.

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

8.7 When a child is under the age of 16 [or younger if the law provides it (up to the age of 13)], the consent of parents will be sought prior to the processing of their data, except when the processing is related to preventative or counselling services offered directly to a child.

9.0 The right to be informed / sharing personal data (privacy notices)

9.1 The privacy notice supplied to individuals in regards to the processing of their personal data will be written in clear, plain language that is concise, transparent, easily accessible, and free of charge.

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

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

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

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

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

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

9.7 In relation to data that is not obtained directly from the data subject, this information will be supplied:

- within one month of having obtained the data
- if disclosure to another recipient is envisaged, at the latest, before the data is disclosed
- if the data is used to communicate with the individual, at the latest, when the first communication takes place

10.0 The right of access

10.1 We shall seek to comply with the rights exercised by data subjects as set out in this section as soon as possible and within legal time limits. However, there may be instances where, due to circumstances outside of our trust's control, this may not be possible, e.g. where the academy or trust has been closed or is only partially operable. In such circumstances, data subjects will be notified and provided with details about the reason for the delay and when a response can reasonably be expected.

10.2 Individuals have the right to obtain confirmation that their data is being processed and the right to submit a data subject access request (DSAR) to gain access to their personal data in order to verify the lawfulness of the processing or obtain copies of their records for other purposes.

10.3 Trust staff should follow our trust's **Data Subject Access Request Procedure.**

10.4 Our website's data protection and GDPR page has guidance for individuals wishing to make a data subject access request.

11.0 The right to rectification

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

11.2 When the personal data in question has been disclosed to third parties, our trust will inform the individual of the rectification where possible.

11.3 When appropriate, our trust will inform the individual about the third parties that the data have been disclosed to.

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

11.5 When no action is being taken in response to a request for rectification, our trust will explain the reason for this to the individual and will inform the individual of his or her right to complain to the supervisory authority and to a judicial remedy.

12.0 The right to erasure

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

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

- when the personal data is no longer necessary in relation to the purpose for which it was originally collected / processed
- when the individual withdraws his or her consent
- when the individual objects to the processing and there is no overriding legitimate interest for continuing the processing
- when the personal data was unlawfully processed
- when the personal data is required to be erased in order to comply with a legal obligation
- when the personal data is processed in relation to the offer of information society services to a child

12.3 Our trust has the right to refuse a request for erasure when personal data are being processed for the following reasons:

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

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

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

12.6 When personal data has been made public within an online environment, our trust will inform other organisations that process the personal data to erase links to and copies of the personal data in question.

13.0 The right to restrict processing

13.1 Individuals have the right to block or suppress our processing of personal data.

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

13.3 Our trust will restrict the processing of personal data in the following circumstances:

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

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

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

14.0 The right to data portability

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

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

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

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

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

14.5 We will provide the information free of charge.

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

14.7 We are not required to adopt or maintain processing systems that are technically compatible with other organisations.

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

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

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

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

15.0 The right to object

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

15.2 Individuals have the right to object to the following types of data processing:

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

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

- an individual's grounds for objecting must relate to his or her particular situation
- we will stop processing the individual's personal data unless the processing is for the establishment, exercise, or defence of legal claims, or when we can demonstrate compelling legitimate grounds for the processing, which override the interests, rights, and freedoms of the individual

16.0 Automated decision making and profiling

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

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

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

17.0 Privacy by design and privacy impact assessments

17.1 We will act in accordance with the UK GDPR by adopting a privacy-by-design approach and implementing technical and organisational measures that demonstrate how we have considered and integrated data protection into processing activities.

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

17.3 DPIAs will allow us to identify and resolve problems at an early stage, thus reducing associated costs, mitigating risk and preventing damage from being caused to our reputation, which might otherwise occur.

17.4 A DPIA screening check will be carried out for all new projects and use of new suppliers. This will determine whether a DPIA is required if the processing is likely to result in a high risk to the rights and freedoms of individuals.

17.5 A DPIA will be used for projects when using new technologies.

17.6 A DPIA will be used for more than one project, when necessary.

17.7 High-risk processing includes but is not limited to the following:

- systematic and extensive processing activities, such as profiling
- large-scale processing of special categories of data or personal data
- systematically monitoring publicly accessible places on a large scale

17.8 We will ensure that all DPIAs include the following information:

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

17.9 When a DPIA indicates high-risk data processing, we will consult the ICO to seek its opinion as to whether the processing operation complies with the UK GDPR.

17.10 Our employees must follow the data protection impact assessment (DPIA) procedure.

18.0 Data breaches

18.1 Our employees should follow the **Trust Data Breach Management Procedure**.

18.2 The term 'personal data breach' refers to a breach of security which has led to the destruction, loss, alteration, unauthorised disclosure of, or access to, personal data.

18.3 Failure to report a breach when required to do so may result in a fine, as well as a fine of up to £17.5 million, or 4% of an organisation's global turnover for the breach itself.

19.0 Third party processors / other authorised persons

19.1 Our trust requires all third party processors, who have access to or process personal data on behalf of our trust, to provide written confirmation that they will comply with the requirements of the UK GDPR and maintain adequate physical and IT security controls to protect our data.

19.2 **We will request contractors, suppliers, and system providers who may process our personal data to provide written assurance to confirm that:**

- any personal data they receive from us in the course of their performance of the relevant contract or service level agreement will only be processed in accordance with our documented instructions
- no personal data will be transferred to any country outside the UK or EU or any international organisation without obtaining our prior written consent
- any of their employees, sub-contractors or other personnel who may be involved in the processing of the personal data are bound by written contractual obligations to keep the personal data confidential.

- no third party will be engaged to carry out any processing activities in respect of the personal data without our prior written consent, and if consent is given, the third party will be subject to a written contract containing the same data protection obligations as set out between you and us in the contract or service level agreement, and the provisions of this policy
- appropriate organisational and technical security measures are in place to protect any personal data, which may be processed or handled under the contract or service level agreement, and to assist us in complying with our obligations to deal with requests from data subjects to exercise their rights under the UK GDPR
- appropriate systems to investigate and report data breaches are in place and that all breaches will be notified to head of governance immediately and the ICO within 72 hours (where relevant)
- contractors / suppliers will assist us in complying with our obligations in relation to security of processing, dealing with data breaches and carrying out privacy impact assessments
- when the services under the contract or service level agreement end, the contractor / supplier will (at our option) delete or return all personal data and copies of the same
- contractors / suppliers will make information demonstrating compliance with the above obligations available to us on request and will allow for and contribute to any audits or inspections that we may conduct. We will seek written confirmation from other authorised persons, e.g. candidates, students, volunteers, contractors, freelancers, members, trustees and local academy board ambassadors that they will comply with our trust and our academies policies and procedures and that we expect appropriate physical and IT data security controls to be exercised if given access to personal data and systems

19.3 Digital data is coded, encrypted, or password-protected, both on a local hard drive and on a network drive that is regularly backed up off-site.

20.0 Data security

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

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

20.3 Digital data is coded, encrypted, or password-protected, both on a local hard drive and on a network drive that is regularly backed up off-site.

20.4 When data is saved on removable storage or a portable device, the device will be kept in a locked filing cabinet, drawer, or safe when not in use.

20.5 Memory sticks are not to be used as a storage device for any personal data that we are accountable for. The use of memory sticks is for read only use.

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

20.7 When possible, our trust enables electronic devices to allow the remote blocking or deletion of data in case of theft.

20.8 Staff, trustees and ambassadors will not use their personal emails for academy purposes. All staff, trustees, members and ambassadors will have a trust email address that should be used for all academy / trust work.

20.9 All necessary members of staff are provided with their own secure login and password. It is expected that all passwords are kept secure, regularly changed and not shared with others.

20.10 Encrypt or password protect personal information on email attachments / devices / memory sticks.

20.11 Circular emails must not be sent to families, even if using the bcc mode.

20.12 **Working away from the school premises – electronic working.** Any information stored on our systems should not be copied outside of the system. This includes saving data on personal devices or personal storage platforms. You must also ensure that when working with personal data away from the school premises, that this is carried out in a secure location and remains confidential, e.g. keeping devices under lock and key. You must also remain vigilant and ensure that confidential conversations cannot be overheard. The person taking the information / devices from our premises accepts full responsibility for the security of data.

20.13 Follow trust data sharing guidance and check there is a legal basis or that we hold a signed privacy notice or data subject access request before sharing personal information about staff and students (and others).

20.13 Under no circumstances are visitors allowed access to confidential or personal information. Visitors to areas of schools and trust offices containing sensitive information must be supervised at all times.

20.14 Academies will ensure that the physical security of the school's buildings and storage systems, and access to them, is reviewed on a regular basis. If an increased risk of vandalism / burglary / theft is identified, extra measures to secure data storage will be put in place.

20.15 Our trust takes its duties under the GDPR seriously, and any unauthorised disclosure may result in disciplinary action.

20.16 The head of governance, the head of IT and executive are responsible for ensuring continuity and recovery measures are in place to ensure the security of protected data.

21.0 Publication of information

21.1 DAT publishes a publication scheme on its website outlining classes of information that will be made routinely available, including:

- policies and procedures
- minutes of meetings
- annual reports
- financial information

21.2 Classes of information specified in the publication scheme are made available quickly and easily on request.

21.3 We will not publish any personal information, including photos, on our website without the permission of the affected individual.

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

22.0 CCTV and photography

22.1 Our trust understands that recording images of identifiable individuals constitutes the processing of personal information, so it is done in line with data protection principles.

22.2 Our trust notifies all pupils, staff, and visitors of the purpose for collecting CCTV images via notice boards, letters, and email.

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

22.4 All CCTV footage will be kept for 30 days for security purposes Further information with regards to CCTV can be found in our trust's CCTV policy.

22.5 Our trust will always indicate its intentions for taking photographs of pupils and will secure permission before publishing them.

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

22.7 Precautions will be taken, as outlined in our online safety policy and acceptable use of information technology in relation to the taking and publishing of students, in print, video or on the school website.

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

Recording of meetings or conversations

22.9 Under data protection legislation, an audio or video recording of a conversation where any individual can be identified from the recording and / or the conversation is the personal data of that individual. You must have an appropriate lawful basis for recording the conversation and individuals must be aware that they are being recorded. Consent will likely be the most relevant basis for processing. If an individual does not know in advance that his or her conversation is being recorded, and a lawful basis for processing has not been identified, then that individual's rights to 'fair and lawful processing' will have been breached

Further information with regards to live streaming of classrooms for virtual / online learning can be found in our online safety policy and acceptable use of information technology.

23.0 Data retention

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

23.2 Unrequired data will be deleted as soon as practicable.

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

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

23.5 Retention periods are outlined in our records management policy.

24.0 DBS data

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

24.2 Data provided by the DBS will never be duplicated.

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

25.0 Policy review

This policy is reviewed every two years by the head of governance. The next scheduled review date for this policy is January 2026