DIXONS ACADEMIES TRUST

GDPR Data Protection Policy

Responsibility for Review: Executive Principal, Dixons Academies Trust
Date of Last Review: November 2021

Contents

1.0 Policy statement

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

DAT 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 governors are aware of their responsibilities and outlines how DAT complies with the following core principles of the GDPR. All employees and volunteers of the DAT must be made aware of the Trust policy and procedures and must provide written acknowledge of their understanding of their individual responsibilities in relation to the GDPR.

All data held by DAT and its academies are the responsibility of the Trust.

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

This policy complies with the requirements set out in the GDPR, which came into effect on 25 May 2018. The government have confirmed that the UK's decision to leave the EU will not affect the commencement of the GDPR.

2.0 Legal framework

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

- the General Data Protection Regulation
- 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
- Trust Protection of Biometric Information policy
- Trust Online Safety Policy and Acceptable Use of Information Technology
- Trust Records Management Policy
- Trust Data Protection Impact Assessments (DPIA) Procedure
- Trust Data Breach Management Procedure
- Trust Data Subject Access Request Procedure
- Trust Data Classification, Handling and Disposal policy
- Data Governance Policy
- Trust Business Continuity Policy (and school local policies)

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:

- E-Security Policy
- Freedom of Information Policy
- Surveillance and CCTV policy

3.0 Controller and Processor

3.1 DAT and Trust schools are both a **"Controller"** and **"Processor"** of personal data. DAT 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, Board Member, and LGB Member. The 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 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 are inaccurate,
- having regard to the purposes for which they are processed, are erased or rectified without delay
- kept in a form that permits identification of data subjects for no longer than is necessary for the purposes for which the personal
- data are 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
- 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).** This is **GDPR Sentry** who are an external provider and duties will include:

- Informing and advising the Trust and employees about their obligations to comply with the GDPR and other data protection laws.
- Monitor the Trust and Trust school's compliance with the GDPR and other laws, including managing internal data protection activities, advising on data protection impact assessments, conducting internal audits, and ensuring the Trust and Trust employees receive appropriate training and data protection awareness communications.

6.2 The Data Protection Officer will report to the Trust Data Protection Lead who will feedback to the highest level of operational management at the Trust, which is the Executive Board.

6.3 The DPO will operate independently and will not be dismissed or penalised for performing his or her task.

6.4 Sufficient resources will be provided to the DPO to enable that person to meet the requisite GDPR obligations.

7.0 Lawful processing

7.1 Under the 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 DAT ensures that consent mechanisms meet the standards of the 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 DPA will be reviewed to ensure it meets the standards of the 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, DAT 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 are not obtained directly from the data subject, information regarding the categories of personal data that DAT 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 are obtained.

9.7 In relation to data that are 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 are disclosed
- if the data are 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 the Trust's control this may not be possible e.g. where the School 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 the **Trust Data Subject Access Request Procedure.** See Flowchart at **Appendix 1.**

10.4 The Trust website 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 have been disclosed to third parties, DAT will inform the individual of the rectification where possible.

11.3 When appropriate, DAT 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, DAT 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 are no longer necessary in relation to the purpose for which they were 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 were unlawfully processed
- when the personal data are required to be erased in order to comply with a legal obligation
- when the personal data are processed in relation to the offer of information society services to a child

12.3 DAT 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 have 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 have been made public within an online environment, DAT 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 DAT's processing of personal data.

13.2 In the event that processing is restricted, DAT 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 DAT 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 DAT has verified the accuracy of the data
- when an individual has objected to the processing and DAT is considering whether its legitimate grounds override those of the individual
- when processing is unlawful and the individual opposes erasure and requests restriction instead
- when DAT no longer needs 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 have been disclosed to third parties, DAT 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 DAT 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 DAT 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 DAT is 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, DAT will consider whether providing the information would prejudice the rights of any other individual.

14.9 DAT 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, DAT 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 DAT 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 are 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
- DAT will stop processing the individual's personal data unless the processing is for the establishment, exercise, or defence of legal claims, or when DAT can demonstrate compelling legitimate grounds for the processing, which override the interests, rights, and freedoms of the individual

15.4 When personal data are processed for direct marketing purposes:

- DAT will stop processing personal data for direct marketing purposes as soon as an objection is received
- DAT cannot refuse an individual's objection regarding data that are being processed for direct marketing purposes

15.5 When personal data are processed for direct marketing purposes:

- the individual must have grounds relating to that person's particular situation in order to exercise his or her right to object
- when the processing of personal data is necessary for the performance of a public interest task, DAT is not required to comply with an objection to the processing of the data

15.6 When the processing activity is outlined above but is carried out online, DAT will offer a method for individuals to object online.

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 DAT 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.

16.3 When automatically processing personal data for profiling purposes, DAT 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 mathematical or statistical procedures
- implementing appropriate technical and organisational measures to enable inaccuracies to be corrected and to 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

16.4 Automated decisions must not concern a child or be based on the processing of sensitive data, unless:

- DAT has the explicit consent of the individual
- the processing is necessary for reasons of substantial public interest on the basis of Union / Member State Law

17.0 Privacy by design and privacy impact assessments

17.1 DAT will act in accordance with the GDPR by adopting a privacy-by-design approach and implementing technical and organisational

measures that demonstrate how DAT has 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 DAT's data protection obligations and meeting individuals' expectations of privacy.

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

17.4 A DPIA will be carried out when using new technologies or when 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 more than one project, when necessary.

17.6 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, which is in relation to criminal convictions or offences

17.7 DAT 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

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

17.9 Trust employees should follow the Trust Data Protection Impact Assessment (DPIA) Procedure – **see flowchart Appendix 2.**

18.0 Data breaches

18.1 Trust employees should follow the **Trust Data Breach Management Procedure** - see flowchart at Appendix 3.

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 Please refer to the Trust Breach Management Procedure for further information.

18.4 Failure to report a breach when required to do so may result in a fine, as well as a fine of up to €20 million, or 4% of an organisations global turnover for the breach itself.

19.0 Third Party Processors / other authorised persons

19.1 The Trust requires all third party processors who have access to or process personal data on behalf of the Trust, to provide written confirmation that they will comply with the requirements of the 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 written assurance provide contract terms to confirm that:-**

- Any personal data you receive from us in the course of your 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 EEA or any international organisation without obtaining our prior written consent.
- Any of your 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 letter.
- 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 GDPR.
- Appropriate systems to investigate and report data breaches are in place and that all breaches will be notified to DAT Trust immediately and the ICO within 72 hours (where relevant).
- You 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, you will (at our option) delete or return all personal data and copies of the same.
- You 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, Board Members, LGB Members that they will comply with Trust and Trust school 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 are 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 are 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 are 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 DAT is 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, DAT enables electronic devices to allow the remote blocking or deletion of data in case of theft.

20.8 Staff and governors will not use their personal emails for academy purposes. All staff and governors 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 change them and don't share with others.

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

20.11 Circular emails to parents are sent blind carbon copy (bcc), so email addresses are not disclosed to other recipients.

20.12 When sending confidential information by fax, staff will always check that the recipient is correct before sending.

20.13 **Working away from the school premises – electronic working.** Any information stored on DAT 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 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 DAT premises accepts full responsibility for the security of data.

20.14 Follow Trust Data Sharing Guidance (Appendix 4) 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).

20.15 Under no circumstances are visitors allowed access to confidential or personal information. Visitors to areas of DAT containing sensitive information are supervised at all times.

20.16 Trust schools 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.

20.17 DAT takes its duties under the GDPR seriously, and any unauthorised disclosure may result in disciplinary action.

20.18 The Trust Data Protection Lead and Executive Board 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 DAT will not publish any personal information, including photos, on its website without the permission of the affected individual.

21.4 When uploading information to a DAT 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 DAT 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 DAT 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; the OPS Manager is responsible for keeping the records secure and allowing access.

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

22.6 If DAT wishes to use images / video footage of pupils in a publication, such as a DAT 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 the Trust 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 the DAT 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 DAT 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 the DAT 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 Trust Data Protection Lead

The next scheduled review date for this policy is January 2023

Appendix 1 - Trust data subject access request procedure

To be used in conjunction with Trust Privacy Notices and Trust Data Sharing Guidance .

Appendix 2 - Trust DPIA procedure flowchart

STAGE 1 – DATA SYSTEM APPROVED

Stage 1 requires sign off by Project Lead / Academy GDPR Lead.

Move on to Stage 2

STAGE 2 – DATA PROTECTION IMPACT ASSESSMENT

DPIA to be completed in GDPR Sentry by Project Lead / Academy GDPR Lead.

Upload relevant project documents in GDPR Sentry

PERIODIC REVIEW

DPIAs should be reviewed periodically by the Trust Data Protection Lead / Project Lead for accuracy and in the event of any changes to the system of processing of data.

Appendix 3 - Trust Data Breach Management Procedure

DATA BREACHES SHOULD BE REPORTED IMMEDIATELY TO

THE ACADEMY (OPERATIONS & BUSINESS MANAGER, HEAD OF IT/PRINCIPAL) AND THE DATA PROTECTION OFFICER (DPO) -
TEL: 0113 8042035 E: support@GDPRsentry.com

GIVE AS MUCH INFORMATION AS POSSIBLE

**THE DATA BREACH WILL BE LOGGED ON GDPR SENTRY
BY THE OPERATIONS AND BUSINESS MANAGER**

**IF DETERMINED TO BE ICO NOTIFIABLE, THE ICO WILL BE NOTIFIED WITHIN 72 HOURS
BY THE DATA PROTECTION OFFICER**

**IN ALL CASES, AN INVESTIGATION WILL BE IMPLEMENTED BY THE
ACADEMY DATA PROTECTION LEAD WITH SUPPORT FROM THE DPO**

**RECOMMENDATIONS FOR IMPROVEMENT WILL BE SHARED AND
CONTROL MEASURES IMPLEMENTED**

Take care when dealing with student and staff data

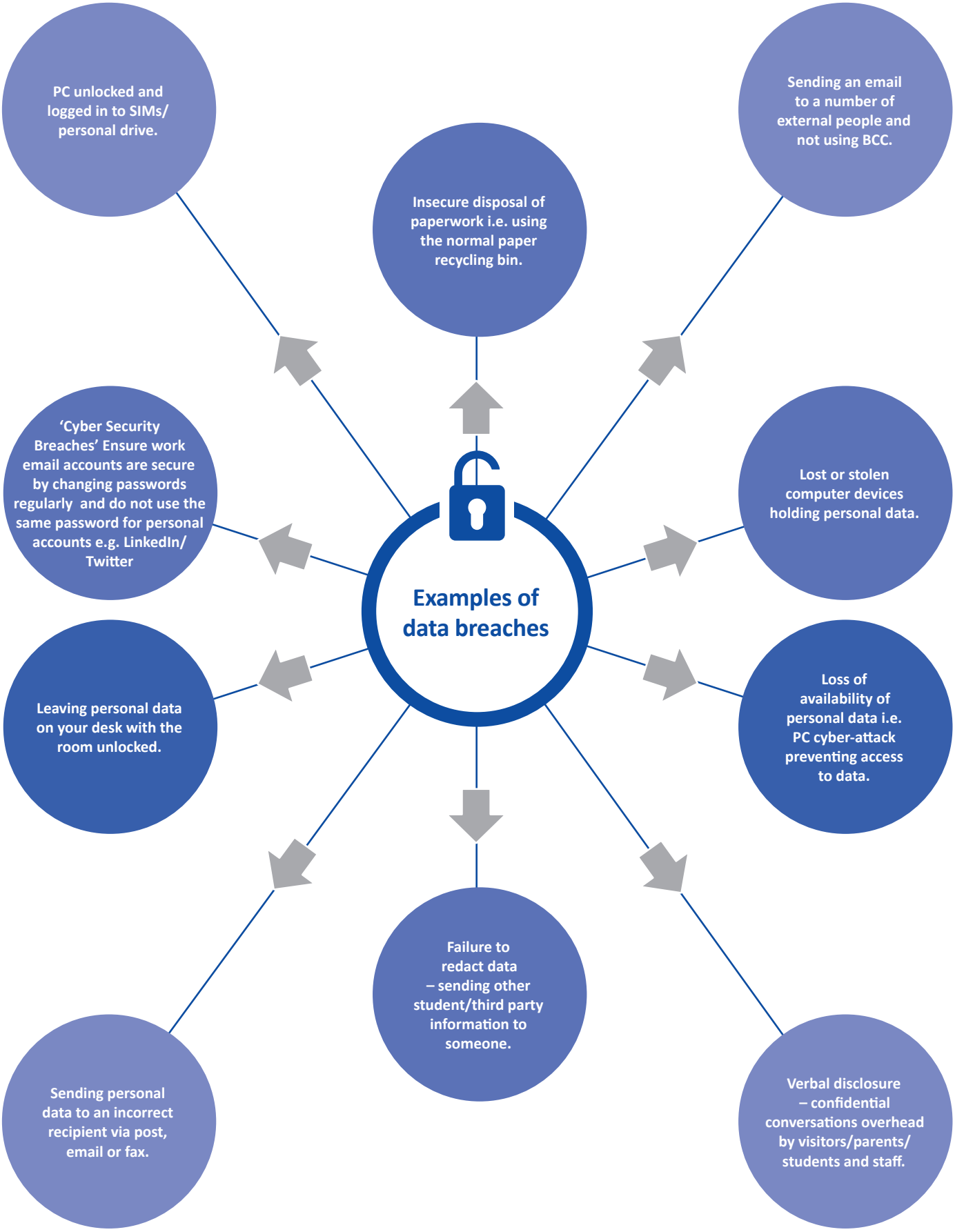
Personal data is an individual's name and any other piece of identifying information – see below for examples of personal data handled in schools.

- Address details
- SEN status
- Free School Meals eligibility
- Pupil Premium
- Educational levels and results (Inc. mock / practice exam papers / pieces of work with comments / feedback)
- Child protection details
- Witness / incident details
- Accident records
- Photographs
- Staff payroll / salary information
- Staff performance management details

Top tips to keep data safe

- Documents containing personal data should be shredded or placed in the confidential waste consoles.
- Do not leave documents printing which contain personal data. If the printer jams, report this immediately and do not leave until the jam has been cleared.
- If something personal is left on the printer, or somewhere public, pass it on to the Operations & Business Manager who will report it to the DPO.
- Take care when using electronic whiteboards in classrooms – registers often show FSM, SEN alerts etc.
- Take care not to inadvertently display other students' results / grades if using lists at Parent Evenings.
- Ensure you confirm the identity of callers and email addresses before discussing personal data.
- Where it is necessary to send data elsewhere, send it securely e.g. encrypted document / email / Secure Access S2S or BSO Dropbox.
- Keep your working area and desk tidy and do not leave documents out for others to see. Always lock away confidential information in a lockable cupboard / filing cabinet.
- Take care not to display personal data if visitors and students regularly use your office.
- Lock your PC / laptop when not in use – especially in classrooms and public areas.
- Do not share your passwords with anyone; keep them safe in a password protected document on your PC / laptop.
- Do not use portable external devices i.e. memory sticks / external hard drives. All documents are to be saved to the desk top / one drive.
- New software requests must be submitted to the IT helpdesk to ensure they are compliant and compatible. The form is available on the SharePoint site under GDPR.
- If you access work emails on your mobile phone, you are responsible to ensure that data cannot be seen or accessed by anyone else. Please remember that most coffee shops i.e. Costa have unsecure Wi-Fi networks.
- When you are sending an email to a number of people outside of the organisation i.e. suppliers, please ensure you put them in BCC (Blind Carbon Copy) so their email addresses are not visible to each other.
- Check the school holds signed Privacy Notices before sharing any data covered by the Privacy Notices.

Examples of data breaches within the school environment



Appendix 4 - Trust data protection – Data Sharing Guidance (SARs)

To ensure that the sharing of Trust and school level data complies with the law the checklists below should be used in conjunction with the following policies and guidance:-

- Trust GDPR Policy and other policies e.g. Freedom of information Policy, Surveillance and CCTV Policy, Trust Online Safety Policy and Acceptable Use of Information Technology, Trust Records Management Policy.
- Trust Data Subject Access Request Procedure
- Trust Data Protection Training
- Students, Parents and Staff Privacy Notice
- ICO Data Sharing Code of Practice – search for latest version at www.ico.org.uk

Please forward Data Protection requests to the Operations and Business Manager. Advice is available from the Data Protection Officer for complex requests.

Data sharing checklists

One off requests	Systematic data sharing
Example: You are asked to share personal data relating to a pupil, family members or member of staff in a 'one off' circumstance e.g. a parent asks for a copy of their child's education records or the school receives a request for data in relation to a criminal investigation.	Example: You want to enter into an agreement to share staff or student personal data on an ongoing basis e.g. MIS Systems and systems//web platforms and apps which link to school MIS Systems or require manual uploads of staff and student data. A Data Protection Impact Assessment (DPIA) needs to be completed – see Academy Operations & Business Manager or IT Infrastructure Manager in first instance.
Is the sharing justified? • Do you think you should share the information? • Have you assessed the potential benefits and risks to individuals and / or society of sharing or not sharing? (e.g. SEN data / Child Protection details) • Have you assessed the potential benefits and risk to individuals and / or society of sharing or not sharing? • Do you have concerns that an individual is at risk of serious harm? • Do you need to consider an exemption in the DPA to share?	**Is the sharing justified?** • What is the sharing meant to achieve? • Have you assessed the potential benefits and risk to individuals and / or society of sharing or not sharing? • Is the sharing proportionate to the issue you are addressing? • Could the objective be achieved without sharing personal data?
Do you have the power to share? • Is the data outlined in the Student / Staff Privacy Notices and has consent been obtained? • The nature of the information you have been asked to share (for example was it given in confidence. E.g. Child Protection details – involved the school DSL). • Any legal obligation to share information (for example a statutory requirement or a court order e.g. Police Section 29 Request or Education Act – The law allows the transfer of pupil data when a child moves schools and to other agencies (as per Privacy Notice).	**Do you have the power to share?** Requests for systems to be linked to school student and staff data should be requested through the Operations and Business Manager who can liaise with the school ICT lead and system supplier to ensure data protection security protocols are adequate.

If you decide to share

What information should you share?

- Only share what is necessary – e.g. redact information if it does not relate directly to individual named in the data request (data subject).
- Distinguish fact from fiction.

How should the information be shared?

- Information must be shared securely e.g. encrypted document / email or via www.gov.uk Secure Access S2S School transfer or BSO Dropbox. Seek advice if you are unsure.
- Ensure you are giving the data to the right person – always check the identity and source of requests.
- Consider whether it is appropriate / safe to inform the individual that you have shared their information.

Record the decision

All requests and decisions should be recorded on the GDPR Sentry System as per the Trust Data Protection and Freedom of Information policy.

If you decide to share

It is good practice to have a data sharing agreement in place. As well as considering the key points above, your data sharing agreement should cover the following issues:

- The organisations that will be involved.
- What you need to tell people about the data sharing and how you will communicate that information.
- Measures to ensure that adequate security is in place to protect the data.
- What arrangements need to be in place to provide individuals with access to their personal data if they request it?
- Agreed common retention periods for the data.
- Processes to ensure secure deletion takes place.

Many reputable systems suppliers will incorporate a Data Sharing Protocol as part of their agreement; schools should make sure this is adequate.

Record the Data Sharing Agreement / Data Protection Impact Assessment

Copy Data Sharing Agreements / DPIAs should be stored with the contract paperwork and added to GDPR Sentry.