Policy A12 – Data Protection (including protection of biometric data of children)

University of Brighton Academies Trust

Contents

1. Aims

1.1 The Trust aims to ensure that all personal data collected about staff, pupils, parents/carers, Trustees, Local Board members, volunteers, visitors and other individuals is collected, stored and processed in accordance with the General Data Protection Regulation (EU) 2016/679 (GDPR) and the Data Protection Act 2018 (DPA 2018).

1.2 This policy applies to all personal data, regardless of whether it is in paper or electronic format.

2. Legislation and guidance

2.1 This policy meets the requirements of the GDPR and the DPA 2018. It is based on guidance published by the Information Commissioner's Office (ICO) on the GDPR.

2.2 It meets the requirements of the Protection of Freedoms Act 2012 when referring to use of biometric data.

2.3 It also reflects the ICO's code of practice for the use of surveillance cameras and personal information.

2.4 In addition, this policy complies with the Trust funding agreement and articles of association.

3. Definitions

Term	Definition
Personal data	Any information relating to an identified, or identifiable, individual. The information must relate to a 'living' individual. This may include the individual's: • Name (including initials) • Identification number • Location data • Online identifier, such as a username It may also include factors specific to the individual's physical, physiological, genetic, mental, economic, cultural or social identity.
Special categories of personal data	Personal data which is more sensitive and so needs more protection, including information about an individual's: • Racial or ethnic origin • Political opinions • Religious or philosophical beliefs • Trade union membership • Genetics • Biometrics (such as fingerprints, retina and iris patterns), where used for identification purposes • Health – physical or mental • Sex life or sexual orientation
Processing	Anything done to personal data, such as collecting, recording, organising, structuring, storing, adapting, altering, retrieving, using, disseminating, erasing or destroying. Processing can be automated or manual.
Data subject	The identified or identifiable individual whose personal data is held or processed.
Data controller	A person or organisation that determines the purposes and the means of processing of personal data.
Data processor	A person or other body, other than an employee of the data controller, who

	processes personal data on behalf of the data controller.
Personal data breach	A breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data.

4. The data controller

4.1 The Trust determines the purpose of processing personal data relating to parents/carers, pupils, staff, Trustees, Local Board members, volunteers, visitors and others, and therefore is a data controller.

4.2 The Trust is registered as a data controller with the ICO and will pay the data protection fee for registration annually to the ICO or as otherwise legally required.

5. Roles and responsibilities

5.1 This policy applies to **all staff** employed by the Trust, including all staff based in the academies and its central teams, and to external organisations or individuals working on behalf of the Trust. Staff who do not comply with this policy may face disciplinary action.

5.2 Board of Trustees

5.2.1 The Board of Trustees has overall responsibility for ensuring compliance with all relevant data protection obligations.

5.3 Data Protection Officer

5.3.1 The Data Protection Officer (DPO) is responsible for advising on the implementation of this policy, monitoring compliance with data protection law, and developing related policies and guidelines where applicable.

5.3.2 The DPO will provide an annual report of their activities directly to the Board of Trustees and, where relevant, report to the board their advice and recommendations on data protection issues.

5.3.4 The DPO's responsibilities are:

- To inform and advise the Trust and its employees about their obligations to comply with the GDPR and other data protection laws.
- To monitor compliance with the GDPR and other data protection laws, including managing internal data protection activities, advise on data protection impact assessments; train staff and conduct internal audits.
- To be the first point of contact for the ICO and for individuals whose data is processed by the Trust

5.3.5 The DPO for the Trust is Samantha Coates, who is supported by a Data Protection Co-ordinator, They are contactable via email privacy@brightonacademiestrust.org.uk.

5.4 Senior Staff

5.4.1 In an academy the Principal acts as the representative of the data controller on a day-to-day basis.

5.4.2 For Professional Services the relevant head of service acts as the data controller on a day to day basis.

5.5 All staff

5.5.1 Staff are responsible for:

- Collecting, storing and processing any personal data in accordance with this policy
- Informing the relevant professional service of any changes to their personal data, such as a change of address
- Completing a Data Processing impact assessment whenever they are engaging in a new activity[1] that may affect the privacy rights of individuals
- Contacting the DPO (via privacy@brightonacademiestrust.org.uk) in the following circumstances:
    - With any questions about the operation of this policy, data protection law, retaining personal data or keeping personal data secure
    - If they have any concerns that this policy is not being followed
    - If they are unsure whether or not they have a lawful basis to use personal data in a particular way
    - If they need to rely on or capture consent, draft a privacy notice, deal with data protection rights invoked by an individual, or transfer personal data outside the European Economic Area
    - If there has been a data breach
    - If they need help with any contracts or sharing personal data with third parties

6. Data protection principles

6.1 The GDPR is based on data protection principles that must be complied with. This policy sets out how the Trust aims to comply with these principles. The principles say that personal data must be:

- Processed lawfully, fairly and in a transparent manner
- Collected for specified, explicit and legitimate purposes
- Adequate, relevant and limited to what is necessary to fulfil the purposes for which it is processed
- Accurate and, where necessary, kept up to date
- Kept for no longer than is necessary for the purposes for which it is processed
- Processed in a way that ensures it is appropriately secure

7. Collecting personal data

7.1 Lawfulness, fairness and transparency

7.1.1 Personal data will only be processed when there is one of 6 'lawful bases' (legal reasons) to do so under data protection law:

- The data needs to be processed so that the Trust can **fulfil a contract** with the individual, or the individual has asked the Trust to take specific steps before entering into a contract
- The data needs to be processed to **comply with a legal obligation**
- The data needs to be processed to ensure the **vital interests** of the individual or another person e.g. to protect someone's life
- The data needs to be processed so that the Trust, as a public authority, can perform a task **in the public interest or exercise its official authority.**

[1] an activity that involves processing of personal data for a purpose that is new or different from current processing

- The data needs to be processed for the **legitimate interests** of the Trust (where the processing is not for any tasks the Trust performs as a public authority) or a third party, provided the individual's rights and freedoms are not overridden.
- The individual (or their parent/carer when appropriate in the case of a pupil) has freely given clear **consent**

7.1.2 For special categories of personal data, we will also meet one of the special category conditions for processing under data protection law:

- The individual (or their parent/carer when appropriate in the case of a pupil) has given **explicit consent**
- The data needs to be processed to perform or exercise obligations or rights in relation to **employment, social security or social protections law**
- The data needs to be processed to ensure the **vital interests** of the individual or another person, where the individual is physically or legally incapable of giving consent
- The data has already been made **manifestly public** by the individual
- The data needs to be processed for the establishment, exercise or defence of **legal claims**
- The data needs to be processed for reasons of **substantial public interest** as defined in legislation
- The data needs to be processed for **health or social care purposes**, and the processing is done by, or under the direction of, a health or social work professional or by any other person obliged to confidentiality under the law.
- The data needs to be processed for **public health reasons**, and the processing is done by, or under the direction of, a health professional or by any other person obliged to confidentiality under law

  The data needs to be processed for **archiving purposes**, scientific or historical research purposes, or statistical purposes, and the processing in the public interest

7.1.3 For criminal offence data, we will meet both a lawful basis and a condition set out under data protection law.
Conditions include:

- The individual (or their parent/carer when appropriate in the case of a pupil) has given **consent**
- The data needs to be processed to ensure the **vital interests** of the individual or another person, where the individual is physically or legally incapable of giving consent
- The data has already been made **manifestly public** by the individual
- The data needs to be processed for or in connection with legal proceedings, to obtain legal advice, or for the establishment, exercise or defence of **legal rights**
- The data needs to be processed for reasons of substantial public interest as defined in legislation

7.1.4 Whenever we first collect personal data directly from individuals, we will provide them with the relevant information required by data protection law.

7.1.5 We will always consider the fairness of our data processing. We will ensure we do not handle personal data in ways that individuals would not reasonably expect, or use personal data in ways which have unjustified adverse effects on them.

7.2 Limitation, minimisation and accuracy

7.2.1 Only personal data for specified, explicit and legitimate reasons will be collected. The reasons for collecting the data will be explained to the individuals when the data is first collected.
If personal data is to be used for reasons other than those given when it was first obtained , the individuals concerned will be informed before it is used and consent sought.

7.2.2 Staff must only process personal data where it is necessary in order to do their jobs.
When staff no longer need the personal data they hold, they must ensure it is deleted .
Anonymisation of data should only be used when deletion is not an option (e.g.backups). This will be done in accordance with the Trust retention schedule.

8. Sharing personal data

8.1 The Trust will not normally share personal data with anyone else, but may do so where:

- There is an issue with a pupil or parent/carer that puts the staff safety at risk
- There is a need to liaise with other agencies – consent will be sought as necessary before doing this
- Suppliers or contractors need data to enable the Trust to provide services to staff and pupils – for example, IT companies. When doing this, the Trust will:
    - Only appoint suppliers or contractors which can provide sufficient guarantees that they comply with data protection law
    - Establish a data sharing agreement with the supplier or contractor, either in the contract or as a standalone agreement, to ensure the fair and lawful processing of any personal data shared between us
    - Only share data that the supplier or contractor needs to carry out their service, and information necessary to keep them safe while working with the Trust

8.2 Personal data will only be shared with law enforcement and government bodies where legally required to do so, including for:

- The prevention or detection of crime and/or fraud
- The apprehension or prosecution of offenders
- The assessment or collection of tax owed to HMRC
- In connection with legal proceedings
- Where the disclosure is required to satisfy safeguarding obligations
- Research and statistical purposes, as long as personal data is sufficiently anonymised or consent has been provided

8.3 Personal data may also be shared with emergency services and local authorities to help them to respond to an emergency situation that affects any of the pupils or staff. Where personal data is transferred to a country or territory outside the European Economic Area, it will be done in accordance with data protection law, specifically in accordance with GDPR Article 45.

9. Subject access requests and other rights of individuals

9.1 Subject access requests

9.1.1 Individuals have a right to make a ‘subject access request’ to gain access to personal information that the Trust holds about them. This includes:

- Confirmation that their personal data is being processed
- Access to a copy of the data
- The purposes of the data processing

- The categories of personal data concerned
- Who the data has been, or will be, shared with
- How long the data will be stored for, or if this is not possible, the criteria used to determine this period
- The source of the data, if not the individual
- Whether any automated decision-making is being applied to their data, and what the significance and consequences of this might be for the individual

9.1.2 Subject access requests can be submitted in any form. A request should include:

- Name of individual
- Contact details to be able to respond to the request (correspondence address/email address/phone number)
- Details of the information requested

9.1.3 If staff receive a subject access request they must immediately forward it to the DPO.

9.1.4 Requests should normally be submitted via the online form SAR request. Alternatively they may be emailed to privacy@brightonacademiestrust.org.uk

9.2 Children and subject access requests

9.2.1 Personal data about a child belongs to that child, and not the child's parents or carers. For a parent or carer to make a subject access request with respect to their child, the child must either be unable to understand their rights and the implications of a subject access request or have given their consent.

9.2.2 Children below the age of 12 are generally not regarded to be mature enough to understand their rights and the implications of a subject access request. Therefore, most subject access requests from parents or carers of pupils in Trust primary academies may be granted without the express permission of the pupil. This is not a rule and a pupil's ability to understand their rights will always be judged on a case-by-case basis.

9.2.3 Children aged 12 and above are generally regarded to be mature enough to understand their rights and the implications of a subject access request. Therefore, most subject access requests from parents or carers of pupils in Trust secondary academies may not be granted without the express permission of the pupil. This is not a rule and a pupil's ability to understand their rights will always be judged on a case-by-case basis.

9.3 Responding to subject access requests

9.3.1 When responding to requests, the Trust:

- May ask the individual to provide 2 forms of identification
- May contact the individual via phone to confirm the request was made
- Will respond without delay and within 1 month of receipt of the request (or receipt of the additional information needed to confirm identity, where relevant)
- Will provide the information free of charge
- May tell the individual we will comply within 3 months of receipt of the request, where a request is complex or numerous. We will inform the individual of this within 1 month, and explain why the extension is necessary

9.3.2 Information will not be disclosed if it:

- Might cause serious harm to the physical or mental health of the pupil or another individual

- Would reveal that the child is at risk of abuse, where the disclosure of that information would not be in the child's best interests
- Would include another person's personal data that we can't reasonably anonymise, and we don't have the other person's consent and it would be unreasonable to proceed without it.
- Is part of certain sensitive documents, such as those related to crime, immigration, legal proceedings or legal professional privilege, management forecasts, negotiations, confidential references or exam scripts

9.3.3 If the request is unfounded or excessive, the Trust may refuse to act on it, or charge a reasonable fee which takes into account administrative costs.

9.3.4 A request will be deemed to be unfounded or excessive if it is repetitive or asks for further copies of the same information.

9.3.5 When refusing a request, the individual will be told why and that they have the right to complain to the ICO.

9.4 Other data protection rights of the individual

9.4.1 In addition to the right to make a subject access request (see above), and to receive information when the Trust are collecting their data about how it is used and processed (see section 7), individuals also have the right to:

- Withdraw their consent to processing at any time
- Ask for their personal data to be rectified, erased, restricted in its processing, (in certain circumstances)
- Prevent use of their personal data for direct marketing
- Object to processing which has been justified on the basis of public interest, official authority or legitimate interests
- Challenge decisions based solely on automated decision making or profiling (decisions taken with no human involvement, that might negatively affect them)
- Prevent processing that is likely to cause damage or distress
- Be notified of a data breach in certain circumstances
- Make a complaint to the ICO
- Ask for their personal data to be transferred to a third party in a structured, commonly used and machine-readable format (in certain circumstances)

9.4.2 Individuals should submit any request to exercise these rights to the DPO. If staff receive such a request, they must immediately forward it to the DPO.

9.5 Parental requests to see the educational record

9.5.1 Parents, or those with parental responsibility, may make a request for access to their child's educational record for pupils/students under the age of 18. The Trust defines the data held on a child's educational record as:

- Records of the pupil's academic achievements;
- Correspondence concerning the pupil from teachers, local authorities, employees and educational psychologists engaged by the academy/Trust;
- Information from the pupil and their parent(s).

It **does not** include information about the pupil:

- That a teacher keeps solely for their own use.
- Provided by the parent of another child.

9.5.2 It should be noted that:

- there is no automatic right to see educational records;
- requests are not covered by the Data Protection Act and are separate from Subject Access Requests;
- Information will not be disclosed if it:
  - Might cause serious harm to the physical or mental health of the pupil or another individual
  - Would reveal that the child is at risk of abuse, where the disclosure of that information would not be in the child's best interests
  - Is contained in adoption or parental order records
  - Is given to a court in proceedings concerning the child
- the law relating to such requests is not regulated by the ICO;
- a response will be given without delay and normally within 15 school days of receipt of the request;
- responses will normally be given via email however, if a physical copy of the information is requested charges may be made for supplying the information as shown below:

Number of pages of information supplied	Maximum fee
1-19	£1
20-29	£2
30-39	£3
40-49	£4
50-59	£5
60-59	£6
70-79	£7
80-89	£8
90-99	£9
100-149	£10
150-199	£15
200-249	£20
250-299	£25
300-349	£30
350-399	£35
400-449	£40
450-499	£45
500+	£50

9.5.2 Requests specifically relating to educational records must be submitted in writing to the DPO.

A request should include:

- Name of pupil/student
- Contact details of the parent/carer to be able to respond to the request (correspondence address/email address/phone number)
- That the request is for an educational record

9.5.3 If staff receive a request for access to an educational record they must immediately forward it to the DPO.

9.5.4 Requests should normally be submitted via the online form SAR request. Alternatively they may be emailed to privacy@brightonacademiestrust.org.uk

10. Biometric recognition systems

10.1 Where pupils' biometric data is used as part of an automated biometric recognition system (for example, pupils use finger prints for cashless catering or to borrow books, the Trust will comply with the requirements of the Protection of Freedoms Act 2012.

10.2 Parents/carers will be notified before any biometric recognition system is put in place or before their child first takes part in it. The academy will get written consent from at least one parent or carer before taking any biometric data from their child and first process it.

10.3 Parents/carers and pupils have the right to choose not to use the academy's biometric system(s). An alternative means of accessing the relevant services will be provided for those pupils. For example, pupils can pay for catering in cash at each transaction if they wish.

10.4 Parents/carers and pupils can object to participation in the academy's biometric recognition system(s), or withdraw consent, at any time, and any relevant data already captured is deleted.

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

10.6 Where staff members or other adults use the academy's biometric system(s), consent will also be obtained before they first take part in it, and an alternative means of accessing the relevant service will be provided if they object. Staff and other adults can also withdraw consent at any time, and the academy will delete any relevant data already captured.

11. CCTV

11.1 CCTV in used in various locations around the Trust's sites to ensure they remain safe. The Trust will adhere to the ICO's code of practice for the use of CCTV.

11.2 An individuals' permission to use CCTV is not required, however, it is made clear where individuals are being recorded. Security cameras are clearly visible and accompanied by prominent signs explaining that CCTV is in use.

11.3 Any enquiries about the CCTV system should be directed to the Trust Estates & Facilities Management Director via email to facilities@brightonacademiestrust.org.uk

12. Photographs and videos

12.1 Academy activities may include photographing and recording images of individuals. Written consent will be obtained from parents/carers for photographs and videos to be taken of their child for communication, marketing and promotional materials.

12.2 In a primary academy it will be clearly explained how the photograph and/or video will be used to both the parent/carer and pupil.

12.3 In a secondary academy, where parental consent is needed (ie as per 12.1), it will be clearly explained how the photograph and/or video will be used to both the parent/carer and pupil. Where parental consent isn't needed, it will be clearly explained to the pupil how the photograph and/or video will be used.

12.4 Any photographs and videos taken by parents/carers at Trust events for their own personal use are not covered by data protection legislation. However, we will ask that photos or videos with other pupils are not shared publicly on social media for safeguarding reasons, unless all relevant parents/carers (or pupils where appropriate) have agreed to this.

12.5 Where the Trust takes photographs and videos, uses may include:

- Within the academy on notice boards and in academy magazines, brochures, newsletters, etc.

- Outside of the academy by external agencies such as the academy photographer, newspapers, campaigns
- Online on the academy website or social media pages

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

12.7 Photographs and videos used in this way will not be accompanied with any other personal information about the child, to ensure they cannot be identified.

12.8 Please refer to Trust policy A14 Photography and Image Sharing for more information on the use of photographs and videos.

13. Data protection by design and default

13.1 Measures will be in place to show that data protection is integrated into all data processing activities, including:

- Appointing a suitably qualified DPO, and ensuring they have the necessary resources to fulfil their duties and maintain their expert knowledge
- Only processing personal data that is necessary for each specific purpose of processing, and always in line with the data protection principles set out in relevant data protection law (see section 6)
- Completing data protection impact assessments where processing of personal data presents a high risk to rights and freedoms of individuals, and when introducing new technologies (the DPO will advise on this process)
- Integrating data protection into internal documents including this policy, any related policies and privacy notices
- Regularly training members of staff on data protection law, this policy, any related policies and any other data protection matters; a record of attendance will be kept
- Regularly conducting reviews and audits to test privacy measures and ensure compliance
- Appropriate safeguards are in place if we were to transfer any personal data outside of the European Economic Area (EEA), where different data protection laws would apply
- Maintaining records of processing activities, including:
    - For the benefit of data subjects, making available the name and contact details for each academy and the Trust DPO and all information the Trust is required to share about how it uses and processes personal data (via privacy notices)
    - For all personal data that is held, maintaining an internal record of the type of data, data subject, how and why the data is being used, any third-party recipients, how and why the data is being stored, retention periods and how the data is kept secure

14. Data security and storage of records

14.1 Personal data will be protected and kept safe from unauthorised or unlawful access, alteration, processing or disclosure, and against accidental or unlawful loss, destruction or damage.
In particular:

- Paper-based records and portable electronic devices, such as laptops and hard drives that contain personal data are kept under lock and key when not in use
- Papers containing personal data must not be left on office and classroom desks, on staffroom tables or left anywhere else where there is general access. An exception to this may be where the well-being of the pupil/student outweighs the individual rights eg specific allergy information – provided documentation exists to justify this decision then this is allowable.
- Where personal information in paper format needs to be taken off site, staff must sign it in and out from the relevant office

- Passwords that are at least 10 characters long containing letters and numbers are used to access Trust computers, laptops and other electronic devices. Staff and pupils are reminded to change their passwords at regular intervals and not use passwords from other sites.
- Encryption is used to protect all portable devices and removable media, such as laptops and USB devices
- Where there is a need to share personal data with a third party, appropriate due diligence will be carried out and reasonable steps taken to ensure it is stored securely and adequately protected (see section 8)
- Staff, pupils or Trustees and Local Board memebrs who store personal information on their personal devices are expected to follow the same security procedures as for school-owned equipment (see our E-Safety Policy/ICT Acceptable use policy and ICT Acceptable use for Students/Pupils policy

15. Disposal of records

15.1 Personal data that is no longer needed will be disposed of securely. Personal data that has become inaccurate or out of date will also be disposed of securely, where there is not a need to rectify or update it.

15.2 For example, paper-based records will be shredded or incinerated, and electronic files overwritten or deleted. A third party may be used to safely dispose of records. If so, the third party will be required to provide sufficient guarantees that it complies with data protection law.

16. Personal data breaches

16.1 All reasonable endeavours will be made to ensure that there are no personal data breaches. In the unlikely event of a suspected data breach, the procedure set out in appendix 1 will be followed.

16.2 When appropriate, the data breach will be reported to the ICO within 72 hours of the moment a breach is identified, including weekends and holidays. Such breaches in an academy context may include, but are not limited to:

- A non-anonymised dataset being published on the academy website which shows the exam results of pupils eligible for the pupil premium
- Safeguarding information being made available to an unauthorised person
- The theft of a Trust laptop containing non-encrypted personal data about pupils
- The loss or theft of paper files or USB containing any personal data

17. Training

17.1 All staff, Trustees and Local Board members are provided with data protection training as part of their induction process.

17.2 Data protection will also form part of continuing professional development, where changes to legislation, guidance or the Trust's processes make it necessary.

18. Monitoring arrangements

18.1 **T**he DPO is responsible for monitoring and reviewing this policy.
This policy will be reviewed annually and shared with the Board of Trustees

19. Links with other policies

This data protection policy is linked to our:

- Academy Safeguarding and Child Protection policy
- Freedom of information publication scheme
- ICT acceptable use policy
- Social Media policy
- Photography and image sharing
- Document retention schedule
- Privacy notices

20. Policy status and review

Written by:	Head of Governance and Admissions/Data Protection Coordinator
Owner:	Data Protection Officer
Status:	V4 = Approved
Approval date:	FRC = 10-05-2018 V2 = 31-05-18 V3 = 03-05-2019 V4 = 02-12-19 Finance and Resources Committee
Review Date:	2021

Appendix 1: 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 the DPO
- 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 alert the Chief Executive Officer/Executive Team and Chair of the Board of Trustees
- The DPO will advise on all reasonable measures to contain and minimise the impact of the breach, assisted by relevant staff members or data processors where necessary.
- 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's 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 it is challenged at a later date by the ICO or an individual affected by the breach. Documented decisions are securely stored within Trust dedicated software.

    Where the ICO must be notified, the DPO will do this via the 'report a breach' page of the ICO website 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 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
    - 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. Documented decisions are recorded in Academies Central: Governance – Governance Documents – Data Protection: Personal Data Breach Procedures: Record of Data Breaches 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)
- The DPO and the responsible senior leader will meet to review what happened and how it can be stopped from happening again. This meeting will happen as soon as reasonably possible

Actions to minimise the impact of data breaches

All actions to mitigate the impact of different types of data breach will be taken, focusing especially on breaches involving particularly risky or sensitive information. The effectiveness of these actions will be reviewed and amended as necessary after any data breach.

The actions that will be taken for different types of risky or sensitive personal data processed by the Trust. For example:

Special category data (sensitive information) being disclosed via email (including safeguarding records)

- If special category data is accidentally made available via email to unauthorized individuals, the sender must attempt to recall the email as soon as they become aware of the error
- Members of staff who receive personal data sent in error must alert the sender and the DPO as soon as they become aware of the error
- If the sender is unavailable or cannot recall the email for any reason, the DPO will ask the ICT department to recall it
- In any cases where the recall is unsuccessful, the DPO will contact the relevant unauthorized individual who received the email, explain that the information was sent in errot, and request that those individuals delete the information and do not share, publish, save or replicate it in any way.
- The DPO will ensure we receive a written response from all the individuals who received the data, confirming that they have complied with this request
- The DPO will carry out an internet search to check that the information has no0t been made public; if it has, we will contact the publisher/website owner or administrator to request that the information is removed from their website and delated