Author	Encarna Aparicio	Target group	All employees, consultants and volunteers
Issued	April 2025		
Approved by	Full Board	Next review	April 2027

Data Protection Policy

Aims and scope

Anthem Schools Trust (the Trust) aims to ensure that all personal data collected about staff, students, parents/carers, Anthem Community Council (ACC) members, Trustees, visitors and other individuals is collected, stored and processed in accordance with UK data protection law.

This policy applies across Anthem including all schools, the National Team, all ACCs, the Executive Team and the Trustees. The policy applies to all personal data, regardless of whether it is in paper or electronic format.

This policy is available via the Anthem website and each school website and on request. This policy can be made available in large print or other accessible formats if required.

Legislation and guidance

This policy meets the requirements of the:

- UK General Data Protection Regulation (UK GDPR) – the EU GDPR was incorporated into UK legislation, with some amendments, by The Data Protection, Privacy and Electronic Communications (Amendments etc) (EU Exit) Regulations 2020
- Data Protection Act 2018 (DPA 2018)

It is based on guidance published by the Information Commissioner's Office (ICO) on the UK GDPR and guidance from the Department for Education (DfE) on Generative artificial intelligence in education.

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

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

In addition, this policy complies with our funding agreement and articles of association.

Definitions

Term	Definition
Personal data	Any information relating to an identified, or identifiable, 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.

The data controller

Anthem processes personal data relating to parents/carers, students, staff, ACC members, Trustees, visitors and others, and therefore is a data controller.

Anthem, as a data controller, pays an annual fee to the ICO, as legally required. This fee includes all schools (schools do not have separate ICO registration).

Roles and responsibilities

This policy applies to **all staff** employed by Anthem as well as all Trustees, ACC members and other volunteers, and to external organisations or individuals working on our behalf. Staff who do not comply with this policy may face disciplinary action.

Trustee board

The Trustee board has overall responsibility for ensuring that Anthem complies with all relevant data protection obligations.

Data Protection Officer (and Deputy)

The Data Protection Officer (DPO) is responsible for overseeing the implementation of this policy, monitoring our compliance with data protection law, and developing related policies and guidelines

where applicable. The DPO is responsible for setting up and maintaining the network of school data protection leads and ensuring an ongoing program of relevant training, support and templates.

The Deputy Data Protection Officer (Deputy DPO) keeps a log of all SARs, FOI requests and data protection breaches. The Deputy DPO is also responsible for reporting serious breaches in line with the data protection breach protocol (see Appendix 1) and monitoring and supporting data Subject Access Requests (SARs), with oversight by the DPO.

All data breaches reported to the ICO are also recorded by the Deputy DPO on the Serious Incident Report which is shared with the CEO and Trustee Board via the Audit & Risk Committee.

The DPO is the first point of contact for the ICO. Our DPO is Claire Pannell, Director of Governance – General Counsel, and is contactable via email on cpannell@anthemtrust.uk

Our Deputy DPO is Encarna Aparicio, contactable via eaparicio@anthemtrust.uk or 0118 2144378.

School data protection lead

Each school has a data protection lead. There is also a data protection lead for the National Team. Contact details for each data protection lead can be found at Appendix 2.

Each school data protection lead acts as the representative of the data controller on a day-to-day basis within their school/National Team. The data protection leads are responsible for overseeing the implementation of this policy in their school/National Team, responding to data subject access requests, FOI requests, creating and maintaining the school/National Team data protection asset register, action plan and data protection log, completing Data Protection Impact Assessments (DPIAs) as necessary, filtering down data protection training and updates and handling and escalating data protection concerns and breaches in line with the data protection breach protocol and keeping the Headteacher up to date regularly regarding data protection matters (see Appendix 1).

The school data protection leads are the first point of contact for any queries relating to data protection within each school/National Team.

All staff and volunteers

Staff and volunteers are responsible for:

- Collecting, storing and processing any personal data in accordance with this policy
- Informing the school of any changes to their personal data, such as a change of address
- Contacting the relevant school or National Team data protection lead (or the DPO in their absence) 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, deal with data protection rights invoked by an individual, or transfer personal data outside the UK.
    - If there has been a data breach.
    - Whenever they are engaging in a new activity that may affect the privacy rights of individuals.
    - If they need help with any contracts or sharing personal data with third parties.

Data protection principles

The UK GDPR is based on data protection principles that our Trust must comply with.

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.

This policy sets out how the Trust aims to comply with these principles.

Collecting personal data

Lawfulness, fairness and transparency

We will only process personal data where we have one of six 'lawful bases' (legal reasons) to do so under data protection law:

- The data needs to be processed so that the school can **fulfil a contract** with the individual, or the individual has asked the school to take specific steps before entering a contract.
- The data needs to be processed so that the school can **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**.
- 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 student) has freely given clear **consent**.

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

- The individual (or their parent/carer when appropriate in the case of a student) 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 protection 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 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 is in the public interest.

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 student) 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.

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

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.

Further information is available within our suite of Privacy Notices, on school and Trust websites.

Limitation, minimisation and accuracy

We will only collect personal data for specified explicit and legitimate reasons. We will explain these reasons to the individuals when we first collect their data.

If we want to use personal data for reasons other than those given when we first obtained it, we will inform the individuals concerned before we do so and seek consent where necessary.

Staff must only process personal data where it is necessary to do their jobs.

We will keep data accurate and, where necessary, up to date. Inaccurate data will be rectified or erased when appropriate.

When staff no longer need the personal data they hold, they must ensure it is deleted or anonymised. This will be done in accordance with the Retaining Records Policy.

Sharing personal data

We will not normally share personal data with anyone else without consent, but there are certain circumstances where we may be required to do so. These include, but are not limited to, situations where:

- There is an issue with a student or parent/carer that puts the safety of our staff at risk.
- We need to liaise with other agencies – we will seek consent as necessary before doing this.
- Our suppliers or contractors need data to enable us to provide services to our staff and students – for example, IT companies. When doing this, we will:

- Only appoint suppliers or contractors which can provide sufficient guarantees that they comply with UK data protection law.
- Establish a contract with the supplier or contractor to ensure the fair and lawful processing of any personal data we share.
- Only share data that the supplier or contractor needs to carry out their service.

We will also share personal data with law enforcement and government bodies where we are legally required to do so.

We may also share personal data with emergency services and local authorities to help them to respond to an emergency that affects any of our students or staff.

Where we transfer personal data internationally, we will do so in accordance with UK data protection law.

Subject access requests and other rights of individuals

Subject access requests

Individuals have a right to make a 'subject access request' to gain access to personal information that the school or Anthem 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.
- Where relevant, the existence of the right to request rectification, erasure or restriction, or to object to such processing.
- The right to lodge a complaint with the ICO or another supervisory authority.
- The safeguards provided if the data is being transferred internationally.

Subject access requests may be submitted in any form, but we may be able to respond more quickly if they are submitted in writing, either by letter or email, to the relevant school or National Team data protection lead (see Appendix 2 for contact details) and include:

- Name of individual.
- Correspondence address.
- Contact number and email address.
- Details of the information requested and timeframes.

If staff receive a subject access request, they must immediately forward it to the relevant school or National team data protection lead, who will inform the Deputy DPO. The school data protection lead keeps a register of all school data subject access requests in a Data Protection Log. The Deputy DPO maintains the Anthem log, as above.

Students and subject access requests

Personal data about a student belongs to that student, and not the student'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.

Students 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 students under the age of 12 will usually be granted without the express permission of the student. Most subject access requests from parents or carers of students aged 12 or older will not be granted without the express permission of the student. This is not a rule and a student's ability to understand their rights will always be judged on a case-by-case basis.

Responding to subject access requests

When responding to requests:

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

Refusing requests

We may not disclose information for a variety of reasons, such as if it:

- might cause serious harm to the physical or mental health of the student or another individual
- would reveal that the student is being or has been abused, or is at risk of abuse, where the disclosure of that information would not be in the student's best interests
- would include another person's personal data that we cannot reasonably anonymise, and we do not 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.

If the request is unfounded or excessive, we may refuse to act on it or charge a reasonable fee to cover administrative costs. We will take into account whether the request is repetitive in nature when making this decision.

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

When we refuse a request, we will tell the individual why and tell them they have the right to request an internal review.

Requesting an internal review

If the requester is not satisfied that we have complied with the UK GDPR in responding to their SAR, they can request an internal review by emailing our Data Protection Officer, Claire Pannell, at cpannell@anthemtrust.uk explaining what they would like us to review.

Internal review requests should be made within 15 school days of receipt of the initial response. We will acknowledge the internal review request and provide a response usually within 30 school days. There may be circumstances where we will require more time to complete an internal review. If that is the case, we will inform the requester accordingly and provide a reasonable target date.

We are not obliged to provide a review if it is requested after more than 15 school days of receipt of the initial response.

If the requester is not satisfied with the outcomes of the internal review, then they have the right to make a complaint to the Information Commissioner's office or seek to enforce their subject access right through the courts. Further information about the process can be found under this link: https://ico.org.uk/make-a-complaint/data-protection-complaints/

Other data protection rights of the individual

In addition to the right to make a subject access request (see above), and to receive information when we are collecting their data about how we use and process it (see *Sharing personal data*), individuals also have the right to:

- Withdraw their consent to processing at any time.
- Ask us to rectify, erase or restrict processing of their personal data (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 (i.e. making decisions or evaluating certain things about an individual based on their personal data with no human involvement)
- 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)

Individuals should submit any request to exercise these rights to the school data protection lead or DPO. If staff receive such a request, they must immediately forward it to the Deputy DPO or DPO.

Biometric recognition systems

Where we use students' biometric data as part of an automated biometric recognition system (for example, students use finger prints to receive school dinners instead of paying with cash), we will comply with the requirements of the Protection of Freedoms Act 2012.

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

Parents/carers and students have the right to choose not to use the school's biometric system(s). We will provide alternative means of accessing the relevant services for those students. Parents/carers and students can withdraw consent, at any time, and we will make sure that any relevant data already captured is deleted.

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

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

CCTV

We use CCTV in various locations around the school sites to ensure the sites remain safe. We will follow the ICO's guidance for the use of CCTV, and comply with data protection principles.

We do not need to ask individuals' permission to use CCTV, but we make it clear where individuals are being recorded. Security cameras are clearly visible and accompanied by prominent signs explaining that CCTV is in use.

Any enquiries about the CCTV system should be directed to the relevant school data protection lead.

Photographs and videos

As part of school activities, we may take photographs and record images of individuals within our schools.

We will obtain written consent from parents/carers, or students aged 18 and over, for photographs and videos to be taken of students for communication, marketing and promotional materials.

Where we need parental consent, we will clearly explain how the photograph and/or video will be used to both the parent/carer and student. Where we do not need parental consent, we will clearly explain to the student how the photograph and/or video will be used.

When the school/Trust takes photos or videos, uses may include:

- Within schools on noticeboards and in school magazines, brochures, newsletters, etc.
- Outside of school by external agencies such as the school photographer, newspapers, campaigns.
- Online on our school websites or social media pages.

Consent can be refused or withdrawn at any time. If consent is withdrawn, we will delete the photograph or video and not distribute it further as soon as is reasonably practicable.

When using photographs and videos in this way we will not accompany them with any other personal information about the student, to ensure they cannot be identified.

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

Artificial intelligence (AI)

Artificial intelligence (AI) tools are now widespread and easy to access. Students, parents/carers, staff and volunteers may be familiar with generative chatbots such as ChatGPT and Google Bard. Anthem recognises that AI has many uses to help students learn but also poses risks to sensitive and personal data.

To ensure that personal and sensitive data remains secure, no one will be permitted to enter such data into unauthorised generative AI tools or chatbots.

If personal and/or sensitive data is entered into an unauthorised generative AI tool, Anthem may treat this as a data breach and will follow the personal data breach procedure outlined in Appendix 1.

Data protection by design and default

We have put measures in place to show that we have integrated data protection into all of our 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.
- Appointing our network of school and National Team data protection leads and providing them with an ongoing program of training, support and resources.
- Rolling out data protection training and updates for all staff, ACC members and Trustees across the Trust in response to changing data protection legislation.
- Completing an audit and data protection action plan for each school and the National Team and putting in place a system to keep these updated and maintained.
- 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.
- Completing Data Protection Impact Assessments (DPIA) where the Trust's 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 conducting reviews and audits to test our privacy measures and make sure we are compliant.
- Appropriate safeguards being put in place if we transfer any personal data outside of the UK, where different data protection laws may apply.
- Maintaining records of our processing activities, including:

    - For the benefit of data subjects, making available the name and contact details of our school data protection leads and DPO and all information we are required to share about how we use and process their personal data (via our privacy notices).
    - For all personal data that we hold, maintaining an internal record of the type of data, type of data subject, how and why we are using the data, any third-party recipients, any transfers outside of the UK and the safeguards for those, retention periods and how we are keeping the data secure.

Data security and storage of records

We will protect personal data and keep it 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 confidential personal data must not be left on office and classroom desks, on staffroom tables, or left anywhere else where there is general access.
- Where personal information needs to be taken off site, staff must sign it in and out from the relevant school office.

- Passwords that are at least 10 characters long containing letters and numbers are used to access school computers, laptops and other electronic devices. Staff and pupils are reminded to change their passwords at regular intervals and not reuse passwords from other sites.
- Encryption software is used to protect all portable devices and removable media, such as laptops and USB devices.
- Students, staff, ACC members or other volunteers 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 and Acceptable use agreement).
- When we need to share personal data with a third party, we carry out due diligence and take reasonable steps to ensure it is stored securely and adequately protected.

Disposal of records

Personal data that is no longer needed will be disposed of securely in line with our Retaining Records Policy. Personal data that has become inaccurate or out of date will also be disposed of securely, where we cannot or do not need to rectify or update it.

For example, we will shred or incinerate paper-based records and overwrite or delete electronic files. We may also use a third party to safely dispose of records on the school's behalf. If we do so, we will require the third party to provide sufficient guarantees that it complies with data protection law.

Personal data breaches

We will make all reasonable endeavours to ensure that there are no personal data breaches.

In the unlikely event of a suspected data breach, we will follow the procedure set out in Appendix 1.

When appropriate, we will report the data breach to the ICO within 72 hours after becoming aware of it. Such breaches in a school context may include, but are not limited to:

- a non-anonymised dataset being published on the school 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 school laptop containing non-encrypted personal data about students.

Recording of telephone calls

All telephone calls with Anthem schools may be recorded for training, quality assurance and establishment of facts purposes. We have notices on our websites, in our Data Protection policy and in all our privacy notices to set this out. We also have included information about this on the automatic voice message for each school and the Trust. Personal data obtained on calls is collected, stored and processed in accordance with data protection legislation as set out in our Data Protection policy.

Training

All staff, Trustees, ACC members and other volunteers are provided with data protection training as part of their induction process.

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

Monitoring arrangements

The Deputy DPO is responsible for monitoring and reviewing this policy.

This policy will be reviewed every two years and updated as necessary and approved by the Full Board.

Links with other policies

This Data Protection Policy is linked to our:

- Retaining Records Policy
- Acceptable Use Agreement
- Freedom of Information Policy and Publication Scheme
- Child Protection and Safeguarding Policy
- Privacy Notices

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 data protection breach, or potential breach, the staff member or data processor must immediately notify the relevant school or National Team data protection lead (see Appendix 2), or the Deputy DPO / DPO in their absence.
- The school or National Team data protection lead (or the Deputy DPO in their absence) will initially investigate the report and 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.
- Staff, Trustees and ACC members will co-operate with the investigation (including allowing access to information and responding to questions). The investigation will not be treated as a disciplinary investigation.
- Where it is clear after an investigation that there has been no breach, the report and outcome of the investigation will be recorded but no further action will be taken. When the school data protection lead finds that there has been a breach, or a potential breach, he or she will report this to the Deputy DPO immediately (or the DPO in their absence) – noting the possible 72-hour deadline. If unsure the school data protection lead will seek advice from the Deputy DPO or DPO.
- The DPO, together with the Deputy DPO and school data protection lead, will make all reasonable efforts to contain and minimise the impact of the breach, assisted by relevant staff members or data processors where necessary. (Actions relevant to specific data types are set out at the end of this procedure).
- The Deputy DPO or DPO will assess the potential consequences, based on how serious they are, and how likely they are to happen.
- The Deputy DPO or DPO will work out whether the breach must be reported to the ICO and the individuals affected. Each breach will be judged on a case-by-case basis. To decide, the Deputy DPO or 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.

- The Deputy DPO or DPO may ask the school data protection lead to complete the ICO breach report form in order to make an assessment as to whether the breach is reportable, or in order to make the report to the ICO.
- If it is likely that there will be a significant risk to people's rights and freedoms, the DPO or Deputy DPO will notify the ICO. The DPO/Deputy DPO may also use the ICO's self-assessment tool on the ICO website or call the ICO breach helpline to decide whether a breach is reportable.
- Where the ICO must be notified, the Deputy DPO or the DPO will do this via the 'report a breach' page of the ICO website or through its breach report line (0303 123 1113) within 72 hours of the school's/National Team's awareness of the breach. As required, the completed report form 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 or Deputy 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 or Deputy DPO expects to have further information. The DPO or Deputy DPO will submit the remaining information as soon as possible.
- If the risk to individuals is high, based on the severity and likelihood of potential or actual impact, the DPO or Deputy DPO will make a decision as to whether it is necessary to promptly inform, in writing, the individuals whose personal data has been breached. This notification will set out:
  - A description, in clear and plain language, of the nature of the personal data breach
  - 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.
- Where there has been a reportable breach, the Deputy DPO, or DPO, will inform the relevant Headteacher, Associate Director of Education and CEO and any other relevant third parties as required such as the ESFA and Ofsted. All reportable breaches will be added to the Serious Incident Log and reported to Trustees.
- With Deputy DPO support, the school data protection lead may need to notify any relevant third parties who can help mitigate the loss to individuals – for example, the police, insurers, banks or credit card companies.
- The Deputy DPO and school data protection lead will document each breach, irrespective of whether it is reported to the ICO, in the Data Protection Log, stored electronically. 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)
  - whether reported to the ICO or not
- For all breaches, school data protection leads will be asked by the DPO or Deputy DPO to review what happened and put in place changes to help avoid a recurrence.
- For reportable breaches, the DPO, Deputy DPO, school data protection lead, and any relevant Headteacher and Associate Director of Education will review what happened and how it can be stopped from happening again. This will happen as soon as reasonably possible.

Actions to minimise the impact of data breaches

We set out below some steps we might take to try and mitigate the impact of different types of data breach if they were to occur, focusing especially on breaches involving particularly risky or sensitive information.

- If special category data (sensitive information) is accidentally made available via email to unauthorised 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 school DP Lead or Deputy DPO as soon as they become aware of the error.
- If the sender is unavailable or cannot recall the email for any reason, the school DP Lead or Deputy DPO will ask the IT Team to attempt to recall it and remove it from the school's email system (retaining a copy if required as evidence).
- In any cases where the recall is unsuccessful or cannot be confirmed as successful, the school DP Led or Deputy DPO will consider whether it's appropriate to contact the relevant unauthorised individuals who received the email, explain that the information was sent in error, and request that those individuals delete the information and do not share, publish, save or replicate it in any way.
- The school DP Lead or Deputy DPO will endeavor to obtain a written response from all the individuals who received the data, confirming that they have complied with this request.
- If safeguarding information is compromised, the school DP Lead or Deputy DPO will inform the Designated Safeguarding Lead and discuss whether the school should inform any, or all, of its local safeguarding partners.

Appendix 2: School data protection leads

School/Unit	School/Unit DP Lead	Contact
Abacus Belsize Primary	Rasa Undaraviciute	RUndaraviciute@gladpark.anthemtrust.uk
Judith Kerr Primary	Rasa Undaraviciute	RUndaraviciute@gladpark.anthemtrust.uk
Gladstone Park Primary	Rasa Undaraviciute	RUndaraviciute@gladpark.anthemtrust.uk
Abbey Woods Academy	Caroline Williams	cwilliams@abbeywoods.anthemtrust.uk
All Saints Junior School	David Phillips	dphillips@anthemtrust.uk
Benjamin Adlard Primary Lincoln Carlton Academy Mount Street Academy	Ash Ottewell	aottewell@lincolncarlton.anthemtrust.uk
Boston West Academy	Louise Fairweather Ceri Braybrook	lfairweather@bostonwest.anthemtrust.uk cbraybrook@bostonwest.anthemtrust.uk
The Deepings School	Louise Witts	LWitts@deepings.anthemtrust.uk
Grampian Primary Academy	Helen Chamberlain	hchamberlain@grampian.anthemtrust.uk
Meadow Park Academy	David Phillips	dphillips@anthemtrust.uk
Oakbank School	Demi Bisoffi	DBisoffi@oakbank.anthemtrust.uk
Oxford Spires Academy	Hayley Munro	HMunro@spires.anthemtrust.uk
Queensbury Academy	Kim Morena	KMorena@queensbury.anthemtrust.uk
St Mark's C of E Academy	Christopher Currie	CCurrie@stmarks.anthemtrust.uk

National Team DP Lead	Encarna Aparicio	eaparicio@anthemtrust.uk