ACCOMPLISH MULTI ACADEMY TRUST – Townville Academy

DATA PROTECTION POLICY

Date	October 2023
Prepared by	Trust
Approved by	Trust Board
Review Date	Annual from original policy date or when there is a change in legislation
Version	1
Changes to document	None

VERSION CONTROL

Version	Revision Date	Revised By	Section Revised

CONTENTS

This is a policy adopted by the Accomplish Multi Academy Trust and its schools (referred to as "the trust")

1 AIMS

Our trust aims to ensure that all personal data collected about staff, pupils, parents, trustees, governors, visitors, and other individuals is collected, stored, and processed in accordance with the UK data protection law.

2 Legislation and Guidance

This policy meets the requirements of:

- 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**. 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 regulation 5 of the **Education (Pupil Information) (England) Regulations 2005**, which gives parents the right of access to their child's educational record. In addition, this policy complies with our funding agreement and articles of association.

3 Definitions

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

Automated Processing: any form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to an individual, in particular to analyse or predict aspects concerning that individual's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location, or movements. profiling is an example of automated processing.

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

Data Controller: The natural or legal person, public authority, agency, or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data. It is responsible for establishing practices and policies in line with the GDPR. The trust is the Data Controller of all personal data relating to its pupils, parents, and staff.

Data Subject: a living, identified or identifiable individual about whom we hold personal data. Data Subjects may be nationals or residents of any country and may have legal rights regarding their personal data.

Data Privacy Impact Assessment (DPIA): tools and assessments used to identify and reduce risks of a data processing activity. DPIA can be conducted as part of Privacy by Design and should be conducted for all major systems or business change programs involving the processing of personal data.

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

EEA: the 28 countries in the EU, and Iceland, Liechtenstein, and Norway

Explicit Consent: consent which requires a very clear and specific statement (not just action)

General Data Protection Regulation (GDPR): General Data Protection Regulation ((EU) 2016/679). Personal data is subject to the legal safeguards specified in the GDPR.

Personal data: Any information relating to an identified or identifiable natural person (data subject) who can be identified, directly or indirectly by reference to an identifier such as a name, identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural, or social identity of that natural person. Personal data includes sensitive personal data and pseudonymised personal data but excludes anonymous data or data that has had the identity of an individual permanently removed. Personal data can be factual (for example, a name, email address, location, or date of birth) or an opinion about that person's actions or behaviour.

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

Personal breaches can be organised into three categories:

- Confidentiality breach – where there is an unauthorised or accidental disclosure of or access to personal data.
- Availability breach – where there is an accidental loss of or access to or destruction of personal data.
- Integrity breach – where there is unauthorised or accidental alteration of personal data.

Privacy by Design: implementing appropriate technical and organisational measures in an effective manner to ensure compliance with the GDPR.

Privacy Notices: separate notices setting out information that may be provided to Data Subjects when the trust collects information about them. These notices may take the form of general privacy statements applicable to a specific group of individuals (for example, trust workforce privacy policy) or they may be stand-alone privacy statements covering processing related to a specific purpose.

Processing: Anything done with personal data, such as collection, recording, structuring, storage, adaptation or alteration, retrieval, use, disclosure, dissemination or otherwise making available, restriction, erasure, or destruction

Processor: A natural or legal person, public authority, agency, or other body which processes personal data on behalf of the data controller

Pseudonymisation or Pseudonymised: replacing information that directly or indirectly identifies an individual with one or more artificial identifiers or pseudonyms so that the person, to whom the data relates, cannot be identified without the use of additional information which is meant to be kept separately and secure.

Trust Day: Any day in which there is a session and pupils are in attendance.

Sensitive Personal Data: information revealing racial or ethnic origin, political opinions, religious or similar beliefs, trade union membership, physical or mental health conditions, sexual life, sexual orientation, biometric or genetic data, and Personal data relating to criminal offences and convictions.

Working Days: Exclude trust holidays and “inset” or training days where the pupils are not present.

4 The Data Controller

Our trust processes personal data relating to parents, pupils, staff, governors, visitors, and others, and therefore is a data controller.

The trust is registered with the ICO and has paid its data protection fee to the ICO, as legally required.

Reference number: **Z2809737**

5 Roles and Responsibilities

This policy applies to all staff employed by our trust, and to external organisations or individuals working on our behalf. Staff who do not comply with this policy may face disciplinary action.

5.1 The Trust Board

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

5.2 Data Protection Officer

The trust has appointed Veritau Ltd to be its Data Protection Officer (DPO). The role of the DPO is to ensure that the school is compliant with GDPR and to oversee data protection procedures. Veritau's contact details are:

Information Governance
Veritau Ltd

County Hall
Racecourse Lane
Northallerton
DL7 8AL

schoolsDPO@veritau.co.uk
01609 53 2526

5.3 The Headteacher

The headteacher acts as the representative of the data controller in individual trusts on a day-to-day basis.

5.4 All Staff

Staff are responsible for:

- Collecting, storing, and processing any personal data in accordance with this policy
- Informing the trust of any changes to their personal data, such as a change of address

Contacting the DPO 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 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

6 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.

7 Collecting Personal Data

7.1 Lawfulness, fairness, and transparency

We will only process personal data where we have 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 so that the trust can comply with a legal obligation.
- The data needs to be processed to ensure the vital interests of the individual or another person. i.e., 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 pupil) has freely given clear consent 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 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.

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.

7.2 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 in order to do their jobs.

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

In addition, 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 trust's record retention schedule.

8 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 pupil 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 pupils – 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 situation that affects any of our pupils or staff.

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

9 Privacy Notices

A privacy notice under the GDPR should include:

- The trust's name and contact details
- The contact details of the DPO.
- The personal data you are collecting & why you are collecting it.
- Where you get the personal data from & who you are sharing it with
- The lawful basis for processing the data.
- How long the data will be held for.
- Transfers to third countries and safeguards.
- Description of the data subjects' individual rights.
- The data subjects right to withdraw consent for the processing of their data.
- How individuals can complain.

The trust will publish an overarching privacy notice, which will be posted on its website, which will provide information about how and why the trust gathers and uses images and shares personal data.

In addition to publication of that notice, the trust will also issue privacy notices, to all parents and pupils, before, or as soon as possible after, any personal data relating to them is obtained. This may simply be an explanation of why the information is being requested and the purpose for which it will be used.

The trust will take appropriate measures to provide information in privacy notices in a concise, transparent, intelligible, and easily accessible form, using clear and plain language.

The trust will issue a minimum of two privacy notices, one for pupil information, and one for workforce information, and these will be reviewed at regular intervals to ensure they reflect current processing and are in line with any statutory or contractual changes.

The privacy notices will be amended to reflect any changes to the way the trust processes personal data.

The privacy notice will include details of how/ if the trust uses CCTV (if applicable), whether it intends to use biometric data and how consent will be requested to do this and include details of the trust's policy regarding photographs and electronic images of pupils.

10 Subject access request and other individual rights of individuals

10.1 Subject Access Request (SAR)

Individuals have the 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.
- 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 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.
- The safeguards provided if the data is being transferred internationally.

Subject access requests can be submitted in any form, but we may be able to respond to requests more quickly if they are made in writing and include:

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

If staff receive a subject access request in any form, they must immediately forward it to their headteacher and DPO.

10.2 Children and subject access requests

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.

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 at our trust 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.

10.3 Responding to subject access requests

When responding to requests, we:

- 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.

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 pupil or another individual.
- Would reveal that the child is being or has been abused, or 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?

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.

When we refuse a request, we will tell the individual why, and tell them they have the right to complain to the ICO or they can seek to enforce their subject access right through the courts.

10.4 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 section 7), 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 DPO. If staff receive such a request, they must immediately forward it to the DPO.

11 Parental requests to see the educational record

Parents, or those with parental responsibility, have a legal right to free access to their child's educational record (which includes most information about a pupil) within 15 trust days of receipt of a written request.

If the request is for a copy of the educational record, the trust may charge a fee to cover the cost of supplying it.

If a request is received to view or receive a copy of the education record, the trust will only disclose the information contained in the record and it is not obliged to disclose any further personal data that it may hold. This right applies as long as the pupil concerned is aged under 18.

There are certain circumstances in which this right can be denied, such as if releasing the information might cause serious harm to the physical or mental health of the pupil or another individual, or if it would mean releasing exam marks before they are officially announced.

12 Biometric recognition systems

We do not currently use biometric recognition systems within our trust. An example would be to use fingerprints to receive trust dinners instead of using an online payment system. We would comply with the requirement of the Protection of Freedoms Act 2012.

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

Parents/carers and pupils would have the right to choose not to use the trust's biometric system. We would provide alternative means of accessing the relevant services for those pupils. For example, pupils could pay for trust dinners using an online payment where available.

Parents/carers and pupils could withdraw consent at any time, and we would make sure that any relevant data already captured is deleted.

As required by law, if a pupil 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 pupil's parent(s)/carer(s)

Where staff members of other adults would use the trust's biometric system(s), we would 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 could also withdraw consent at any time and the trust will delete any relevant data captured.

Note: that in the context of the Protection of Freedoms Act 2012, a "child" means a person under the age of 18.

13 CCTV

We use CCTV in various locations around the trust site to ensure it remains 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.

14 Photographs and Videos

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

We will obtain written consent from parents/carers for photographs and videos to be taken of their child for communication, marketing and promotional materials. We will clearly explain how the photograph and/or video will be used to both the parent/carer and pupil.

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 the relevant parents/carers have agreed to this.

Where the trust takes photographs and videos, uses may include:

- Within trusts on notice boards and in trust magazines, brochures, newsletters, etc.
- Outside of the trust by external agencies such as the trust photographer, newspapers, campaigns
- Online on our trust website 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.
- When using photographs and videos in this way we will not accompany them with any other personal information about the child, to ensure they cannot be identified.

15 Artificial Intelligence (AI)

Artificial intelligence (AI) tools are now widespread and easy to access. Staff, pupils and parents/carers may be familiar with generative chatbots such as ChatGPT and Google Bard. The trust recognises that AI has many uses to help pupils 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, the trust will treat this as a data breach, and will follow the personal data breach procedure outlined in appendix 1.

16 Data protection by design and default

We will 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.
- 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 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 training members of staff on data protection law, this policy, any related policies and any other data protection matters; we will also keep a record of attendance.
- 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 trust 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.

17 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.

The use of USBs and any external hard drives will not be permissible within trust for staff/governors/volunteers.

In particular:

- Paper-based records and portable electronic devices, such as laptops/iPad are kept under lock and key when not in use.
- Where personal information needs to be taken off site, staff must sign it in and out from from the trust office.
- Staff and pupils are reminded that they should not reuse passwords from other sites.
- Encryption software is used to protect all portable devices and removable media, such as laptops.
- Staff, pupils or governors who store personal information on their personal devices are expected to follow the same security procedures as for trust-owned equipment (see our Acceptable Use Policy).
- Where 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 (see section 8)
- 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.

18 Disposal of records

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 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 trust's behalf. If we do so, we will require the third party to provide sufficient guarantees that it complies with data protection law.

19 Personal data breaches

The trust 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 trust context may include, but are not limited to:

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

- A non-anonymised dataset being published on the trust 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.

20 Training

All staff, governors and volunteers are provided with data protection training as part of their induction process and no less than annually. More frequent training and briefings will be encouraged, to create a culture of data security and awareness, and where new guidance is introduced.

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

21 Monitoring Arrangements

The headteacher is responsible for monitoring and reviewing this policy.

This policy will be reviewed annually and approved by the trust board

Note: the annual review frequency here reflects the Department for Education's recommendation in its **advice on statutory policies**.

22 Links with other policies

This data protection policy is linked to:

This Policy should be read in conjunction with the following policies:

- Acceptable Use
- Information Governance
- Publication Scheme and FOI
- Records Management and Retention Schedule
- Whistleblowing

Appendix 1: Personal Data Breach

This procedure is based on **guidance on personal data breaches** produced by the Information Commissioner's Office (ICO).

On finding or causing a breach, or potential breach, the staff member, or data processor must immediately notify the data protection officer (DPO) and head teacher

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

Staff will cooperate with the investigation (including allowing access to information and responding to questions). The investigation will not be treated as a disciplinary investigation.

If a breach has occurred or it is considered to be likely that is the case, the DPO will alert the headteacher.

The DPO will make all reasonable efforts to contain and minimise the impact of the breach. Relevant staff members or data processors should help the DPO with this where necessary, and the DPO should take external advice when required (e.g., from IT providers).

The DPO will assess the potential consequences (based on how serious they are and how likely they are to happen) before and after the implementation of steps to mitigate the consequences.

The DPO will work out whether the breach must be reported to the ICO and the individuals affected using the ICO's **self-assessment tool.**

The DPO will document the decisions (either way) in case the decisions are challenged at a later date by the ICO, or an individual affected by the breach.

Where the ICO must be notified, the DPO will do this via the '**report a breach**' page of the ICO website, or through its breach report line (0303 123 1113), within 72 hours of the trust's awareness of the breach.

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 of the trust's awareness of the breach. 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.

Where the trust is required to communicate with individuals whose personal data has been breached, the DPO will tell them in writing.

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..

The DPO will consider, in light of the investigation and any engagement with affected individuals, whether 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 DPO will document each breach, irrespective of whether it is reported to the ICO. For each breach, this record will include the:

- Facts and cause
- Effects
- Action taken to contain it and ensure it does not happen again (such as establishing more robust processes or providing further training for individuals)
- The DPO and the head teacher will meet to review what happened and how it can be stopped from happening again. This meeting will happen as soon as reasonable possible.

Actions to minimise the impact of data breaches

We set out below the 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. We will review the effectiveness of these actions and amend them as necessary after any data breach.

Set out the relevant actions you will take for different types of risky or sensitive personal data processed by your trust. For example:

- Sensitive information being disclosed via email (including safeguarding records).
- 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 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/external IT support provider] to attempt to recall it.
- In any cases where the recall is unsuccessful or cannot be confirmed as successful, the DPO will consider whether it is 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 DPO will endeavour to obtain 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 not 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 deleted.
- If safeguarding information is compromised, the DPO will inform the designated safeguarding lead and discuss whether the trust should inform any, or all of its safeguarding partners.