Data Protection & Information Policy

First Published: September 2018 **Review Date:** March 2022

Trust Board Approval: March 2019 **Last Updated:** August 2019

---

1. Aims

Turner Schools aim to ensure that all personal data collected about staff, pupils, students, parents, carers, governors, visitors and other individuals is collected, stored and processed in accordance with the General Data Protection Regulation (GDPR) and the expected provisions of the Data Protection Act 2018 (DPA 2018) as set out in the Data Protection Bill.

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

2. Legislation and guidance

This policy meets the requirements of the GDPR and the expected provisions of the DPA 2018. It is based on guidance published by the Information Commissioner's Office (ICO) on the GDPR and the ICO's code of practice for subject access requests.

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 code of practice 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

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

Turner Schools processes personal data relating to parents, carers, pupils, students, staff, governors, visitors and others, and therefore is a data controller.

Turner Schools is registered as a data controller with the ICO and will renew this registration annually or as otherwise legally required.

5. Roles and responsibilities

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

5.1 Governing board

The governing board has overall responsibility for ensuring that Turner Schools complies with all relevant data protection obligations.

5.2 Data protection officer
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.

They will provide an annual report of their activities directly to the governing board and, where relevant, report to the board their advice and recommendations on trust data protection issues.

The DPO is also the first point of contact for individuals whose data Turner Schools processes, and for the ICO. Full details of the DPO's responsibilities are set out in their job description.
Our DPO is contactable via DPO@turnerschools.com.

5.3 Headteacher
The headteacher/principal acts as the representative of the data controller 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 Turner Schools 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 European Economic Area
    - 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 GDPR is based on data protection principles that we 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 Turner Schools 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 Turner Schools can **fulfil a contract** with the individual, or the individual has asked Turner Schools to take specific steps before entering into a contract
- The data needs to be processed so that Turner Schools can **comply with a legal obligation**
- The data needs to be processed to ensure the **vital interests** of the individual e.g. to protect someone's life

- The data needs to be processed so that Turner Schools, as a public authority, can perform a task **in the public interest,** and carry out its official functions
- The data needs to be processed for the **legitimate interests** of Turner Schools 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/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 in the GDPR and Data Protection Act 2018.

If we offer online services to pupils/students, such as classroom apps, and we intend to rely on consent as a basis for processing, we will get parental consent (except for online counselling and preventive services).

If we offer online services to pupils/students, such as classroom apps, and we intend to rely on consent as a basis for processing, we will get parental consent where the student is under 13 (except for online counselling and preventive services).
Whenever we first collect personal data directly from individuals, we will provide them with the relevant information required by data protection law.

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.
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 our Retention Policy.

8. Sharing personal data
We will not normally share personal data with anyone else, but may do so where:
- There is an issue with a pupil/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 pupils/students– for example, IT companies. When doing this, we 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 we share
    - Only share data that the supplier or contractor needs to carry out their service, and information necessary to keep them safe while working with us

We will also share personal data with law enforcement and government bodies where we are 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 our safeguarding obligations
- Research and statistical purposes, as long as personal data is sufficiently anonymised or consent has been provided

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, students or staff.

Where we transfer personal data to a country or territory outside the European Economic Area, we will do so in accordance with data protection law.

9. Subject access requests and other rights of individuals

9.1 Subject access requests

Individuals have a right to make a 'subject access request' to gain access to personal information that the school 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 isn't 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

Subject access requests must be submitted in writing, either by letter or email to the DPO. They should include:

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

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

9.2 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 and students at our settings may be granted without the express permission of the pupil or student. This is not a rule and a pupil/student's ability to understand their rights will always be judged on a case-by-case basis.

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/students at our settings may not be granted without the express permission of the pupil or student. This is not a rule and a pupil/student's ability to understand their rights will always be judged on a case-by-case basis.

9.3 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
- 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 will not disclose information if it:

- Might cause serious harm to the physical or mental health of the pupil/student 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

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

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 complain to the ICO.

Individuals are entitled to submit subject access requests all year round, but it may be necessary for us to extend the response period when requests are submitted over the summer holidays. This is in accordance with article 12(3) of the GDPR, and will be the case where the request is complex – for example, where we need multiple staff to collect the data.

9.4 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, or object to the processing of it (in certain circumstances)
- Prevent use of their personal data for direct marketing
- Challenge processing which has been justified on the basis of public interest
- Request a copy of agreements under which their personal data is transferred outside of the European Economic Area
- Object to 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)

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.

10. 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 or student) within 15 school days of receipt of a written request.

11. Biometric recognition systems

Where we use pupil/student's biometric data as part of an automated biometric recognition system (for example, pupils/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. Turner Schools 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 pupils/students can object to participation in a biometric recognition system(s), or withdraw consent, at any time, and we will make sure that any relevant data already captured is deleted. As required by law, if a pupil or 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 pupil or students' parent(s)/carer(s).

Where staff members or other adults use the 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 Turner Schools will delete any relevant data already captured.

12. CCTV

We use CCTV in various locations around the school site to ensure it remains safe. We will adhere to the ICO's code of practice for the use of CCTV.

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 Director of Finance & Operations DFO@turnerschools.com.

13. Photographs and videos

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

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/student.

We will obtain written consent from parents/carers, or students aged 18 and over, for photographs and videos to be taken of pupils and 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 pupil/student. Where we don't need parental consent, we will clearly explain to the pupil/student how the photograph and/or video will be used.

Uses may include:

- Within our settings on notice boards and in school/academy magazines, brochures, newsletters, etc.
- Outside of our settings by external agencies such as the school/academy photographer, newspapers, campaigns
- Online on our setting and 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.

See our Safeguarding Policy more information on our use of photographs and videos.

14. 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 privacy impact assessments where Turner Schools 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
- Maintaining records of our processing activities, including:
    - For the benefit of data subjects, making available the name and contact details of our school 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, data subject, how and why we are using the data, any third-party recipients, how and why we are storing the data, retention periods and how we are keeping the data secure

15. 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, pinned to notice/display boards, 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 school office
- Passwords that are at least 8 characters long containing letters and numbers are used to access school computers, laptops and other electronic devices. Staff and pupils/students are reminded to change their passwords at regular intervals
- Encryption software is used to protect all portable devices and removable media, such as laptops and USB devices
- Staff, pupils/students or governors who store personal information on their personal devices are expected to follow the same security procedures as for trust-owned equipment as per 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)

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

17. Personal data breaches

Turner Schools 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. Such breaches in an education context may include, but are not limited to:

- A non-anonymised dataset being published on the school/academy website which shows the exam results of pupils/students eligible for the pupil premium
- Safeguarding information being made available to an unauthorised person
- The theft of trust laptop containing non-encrypted personal data about pupils/students

18. Training

All staff and governors 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 Turner Schools processes make it necessary.

19. Monitoring arrangements

The DPO is responsible for monitoring and reviewing this policy.
This policy will be reviewed and updated if necessary when the Data Protection Bill receives royal assent and becomes law (as the Data Protection Act 2018) – if any changes are made to the bill that affect Turner Schools practice. Otherwise, or from then on, this policy will be reviewed **every 3 years** and shared with the full governing board.

20. Links with other policies

- Privacy Notice Parents – Use of Child's Data
- Privacy Notice Parents – Use of your own data
- Privacy Notice Pupils & Students
- Privacy Notice School Faculty
- Safeguarding Policy

21. Handling and disclosure of non-personal information

21.1. Rights of access to non-personal information

1. The Trust is a public authority for the purposes of the Freedom of Information Act, and as such the public have a general right of access to information held by the Trust, subject to certain exemptions.
2. The Trust is also required to adopt a publication scheme, setting out information it will pro-actively publish.
3. The Trust is also a public authority for the purposes of the Environmental Information Regulations, which gives access to environmental information.

21.2. Making freedom of information requests

1. In many circumstances, information may be shared informally as part of the Trust's normal working practices. Where more detailed or sensitive information is required it should be treated as a formal Freedom of Information request, or where relevant, a request under the Environmental Information Regulations.
2. Requests for information that includes the personal data of the applicant should be treated as a data protection subject access request, rather than under freedom of information provisions.
3. Formal requests for information must be made in writing, which includes email. There is no need to use a specific form.
4. Requests may be made in the first instance to a school or academy or the Trust centrally. Once received, all requests must be forwarded to the Trust's Data Protection Officer for validation and processing within 3 working days of receipt.
5. A fee may be payable for fulfilling a request. Requests may be refused if complying with them would exceed processing limits set by legislation, or if the information is exempt from disclosure.

21.3. Handling a request

1. Where processing a Freedom of Information request would exceed the cost limits set by legislation, the Trust may refuse the request. In other cases, the Trust may charge disbursement costs as set out in our publication scheme.
2. For requests under the Environmental Information Regulations, the Trust will charge for reasonable staff time required to collate the information in addition to any disbursement costs, as set out in our publication scheme.

3. Where a charge is to be applied we will issue a fees notice and require payment prior to completing the request.
4. For schools, the standard time limit for a Freedom of Information request is 20 school days, or 60 working days if this is shorter. Requests should normally be processed within this time.
5. Under the Environmental Information Regulations, the limit is 20 working days or 40 working days for particularly complex requests.

21.4. Exemptions when disclosing information

1. The right to access relates to information, not documents, so the Trust is not generally obliged to provide copies of original documents - only the relevant information within them.
2. Both the Freedom of Information Act and Environmental Impact Regulations allow exemptions as to the provision of some information, such as where disclosing information would not be in the public interest.
3. Where information has provided by the police, local authority, health care professional or another school, their advice should normally be obtained before disclosing the information.
4. Where redaction (information blacked out/removed) has taken place then a full copy of the information provided should be retained privately by the Trust in order to establish, if a complaint is made, what was redacted and why.

24.5. Providing meaningful information

1. Information disclosed should be clear, thus any codes or technical terms will need to be clarified and explained. If information contained within the disclosure is difficult to read or illegible, then it should be retyped.
2. It may be useful for information to be provided at a face to face meeting, with a relevant member of staff on hand to help and explain matters if requested, or provided at face to face handover.
3. The views of the applicant should be taken into account when considering the method of delivery.

24.6. Freedom of Information Act publication scheme for academies

1. This generic model publication scheme has been prepared and approved by the Information Commissioner. It has been adopted by the Trust and is reproduced at Appendix 2.
2. The scheme commits the Trust:
    a. To proactively publish or otherwise make available as a matter of routine, information, including environmental information, which is held by the authority and falls within the classifications below.
    b. To specify the information which is held by the authority and falls within the classifications below.
    c. To proactively publish or otherwise make available as a matter of routine, information in line with the statements contained within this scheme.
    d. To produce and publish the methods by which the specific information is made routinely available so that it can be easily identified and accessed by members of the public.
    e. To review and update on a regular basis the information the authority makes available under this scheme.
    f. To produce a schedule of any fees charged for access to information which is made proactively available.
    g. To make this publication scheme available to the public
3. Classes of information
    a. Who we are and what we do: Organisational information, locations and contacts, constitutional and legal governance.
    b. What we spend and how we spend it: Financial information relating to projected and actual income and expenditure, tendering, procurement and contracts.
    c. What our priorities are and how we are doing: Strategy and performance information, plans, assessments, inspections and reviews.
    d. How we make decisions: Policy proposals and decisions. Decision making processes, internal criteria and procedures, consultations.
    e. Our policies and procedures: Current written protocols for delivering our functions and responsibilities.

f. Lists and registers: Information held in registers required by law and other lists and registers relating to the functions of the authority.
g. The Services we offer: Advice and guidance, booklets and leaflets, transactions and media releases. A description of the services offered.

4. The classes of information will not generally include:
    a. Information the disclosure of which is prevented by law, or exempt under the Freedom of Information Act, or is otherwise properly considered to be protected from disclosure.
    b. Information in draft form.
    c. Information that is no longer readily available as it is contained in files that have been placed in archive storage, or is difficult to access for similar reasons.
5. The authority will indicate clearly to the public what information is covered by this scheme and how it can be obtained.
6. Where it is within the capability of a public authority, information will be provided on a website. Where it is impracticable to make information available on a website or when an individual does not wish to access the information by the website, a public authority will indicate how information can be obtained by other means and provide it by those means.
7. In exceptional circumstances some information may be available only by viewing in person. Where this manner is specified, contact details will be provided. An appointment to view the information will be arranged within a reasonable timescale.
8. Information will be provided in the language in which it is held or in such other language that is legally required. Where an authority is legally required to translate any information, it will do so.
9. Obligations under disability and discrimination legislation and any other legislation to provide information in other forms and formats will be adhered to when providing information in accordance with this scheme.
10. The purpose of this scheme is to make the maximum amount of information readily available at minimum inconvenience and cost to the public. Charges made by the authority for routinely published material will be justified and transparent and kept to a minimum.
11. Material which is published and accessed on a website will be provided free of charge.
12. Charges may be made for information subject to a charging regime specified by Parliament. Charges may be made for actual disbursements incurred such as:
    a. Photocopying
    b. postage and packaging
    c. the costs directly incurred as a result of viewing information
        1. Charges may also be made for information provided under this scheme where they are legally authorised, they are in all the circumstances, including the general principles of the right of access to information held by public authorities, justified and are in accordance with a published schedule or schedules of fees which is readily available to the public.
        2. If a charge is to be made, confirmation of the payment due will be given before the information is provided. Payment may be requested prior to provision of the information.
        3. Written requests
        4. Information held by a public authority that is not published under this scheme can be requested in writing, when its provision will be considered in accordance with the provisions of the Freedom of Information Act.
        5. Requests should be made to Turner Schools, 4 Westbrook House, 58-60 Shorncliffe Road, Folkestone, CT20 2NQ
13. If a requestor is not satisfied with the outcome of their request, they have a right of complaint via internal review.
    a. Internal review requests must be made in writing to the Data Protection Officer, Turner Schools, 4 Westbrook House, 58-60 Shorncliffe Road, Folkestone, CT20 2NQ or vie email dpo@turnerschools.com
    b. The requestor has a right to complain to the Information Commissioner under section 50 if they are still dissatisfied following the outcome of the Trust's internal review.

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 CEO, appropriate headteacher and the chair of governors
- The DPO 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 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 stored securely on the DPO's Trust laptop.
- 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. 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)
- Records of all breaches will be stored securely on the DPO's Trust laptop.
- The DPO, CEO and appropriate headteacher 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

We will take the actions set out below to mitigate the impact of different types of data breach, 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.

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 to recall it
- In any cases where the recall is unsuccessful, the DPO will 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 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 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

Appendix 2: Publication Scheme

Information to be published	How the information can be obtained	Cost
Class 1 - Who we are and what we do (Organisational information, structures, locations and contacts)		
Who's who in the school	Website	Free
Who's who on the governing body / board of governors and the basis of their appointment	Website	Free
Instrument of Government / Articles of Association	Website	Free
Contact details for the principal and for the governing body, via the school	Website	Free
School prospectus	Website Hard copy	Free
School session times and term dates	Website	Free
Address of school and contact details, including email address.	Website	Free
Class 2 – What we spend and how we spend it (Financial information relating to projected and actual income and expenditure, procurement, contracts and financial audit)		
Annual budget plan and financial statements	Website	Free
Capital funding	Website	Free
Financial audit reports	Website	Free
Governors' allowances that can be incurred or claimed, and a record of total payments made to individual governors.	Website	Free

Class 3 – What our priorities are and how we are doing (Strategies and plans, performance indicators, audits, inspections and reviews)		
Performance management policy and procedures adopted by the governing body.	Website	Free
Performance data or a direct link to it	Website	Free
Ofsted inspection reports	Website	Free
The school's future plans; for example, proposals for and any consultation on the future of the school, such as a change in status	Website	Free
Safeguarding and child protection	Website	Free
Class 4 – How we make decisions (Decision making processes and records of decisions)		
Admissions policy	Website	Free
Agendas and minutes of meetings of the governing body and its committees. (NB this will exclude information that is properly regarded as private to the meetings).	Website	Free
Class 5 – Our policies and procedures (Current written protocols, policies and procedures for delivering our services and responsibilities)		
Records management and personal data policies	Website	Free
Charging regimes and policies.	Website	Free

Class 6 – Lists and Registers		
Asset register	By inspection	Free
Any information the school is currently legally required to hold in publicly available registers	By inspection	Free
Funded Pupil Numbers - post the January Census	Website	Free
Class 7 – The services we offer (Information about the services we offer, including leaflets, guidance and newsletters produced for the public and businesses)		
Extra-curricular activities	Website	Free
Out of school clubs	Website	Free
Services for which the school is entitled to recover a fee, together with those fees	Website	Free
School publications, leaflets, books and newsletters	Website	Free

Schedule of charges

Charge	Description	Basis of charge
Disbursement cost	Photocopying/printing @ 10p per sheet (black & white)	Actual cost
	Photocopying/printing @ 20p per sheet (colour)	Actual cost
	Postage	Actual cost of Royal Mail standard 2nd class
Statutory fees		In accordance with the relevant legislation

Retention schedule

Document type	Basis for retention	Period
COMPANY RECORDS		
Company Articles of Association, Rules / bylaws	Companies Act 2006 Charities Act 2011	Permanent
Academy funding agreement and any supplemental agreements	Charities Act 2011	Permanent
Trustee / director minutes of meetings and written resolutions	Companies Act 2006 Charities Act 2011	10 years
Members' meetings etc. Minutes / resolutions	Companies Act 2006 Charities Act 2011	10 years
Documents of clear historical / archival significance	Data Protection regulation	Permanent if relevant data protection regulation provisions are met.
Contracts eg. with suppliers or grant makers	Limitation Act 1980	Length of contract term plus 6 years
Contracts executed as deeds	Limitation Act 1980	Length of contract term plus 12 years
Intellectual property records and legal files re provision of service	Limitation Act 1980	Life of service provision or IP plus 6 years
TAX AND FINANCE		
Annual accounts and review (including transferred records on amalgamation)	Companies Act 2006 Charities Act 2011	6 years
Tax and accounting records	Finance Act 1998 Taxes Management Act 1970	6 years from end of relevant tax year
Information relevant for VAT purposes	Finance Act 1998 and HMRC Notice 700/21	6 years from end of relevant period
Banking records / receipts book/sales ledger	Companies Act 2006 Charities Act 2011	6 years from transaction

EMPLOYEE / ADMINISTRATION		
Payroll / Employee / Income Tax and NI records: P45; P6; PIID; P60, etc.	Taxes Management Act 1970 / IT (PAYE) Regulations	6 years from end of current year
Maternity pay	Statutory Maternity Pay Regulations	3 years after the end of the tax year
Sick pay	Statutory Sick Pay (General) Regulations	3 years after the end of the tax year
National Minimum wage records	National Minimum Wage Act	3 years after the end of the tax year
Foreign national ID documents	Immigration (Restrictions on Employment) Order 2007 Independent School Standards Regulations	Minimum 2 years from end of employment
HR files and training records	Limitation Act 1970 and Data Protection regulation	6 years from end of employment
Records re working time	Working Time Regulations 1998 as amended	2 years
Job applications (CVs and related materials re unsuccessful applicants)	ICO Employment Practices Code (Recruitment & Selection) Disability Discrimination Act 1995 & Race Relations Act 1976	12 months from your notification of outcome of application
Pre-employment / volunteer vetting	ICO Employment Practice Code Independent School Standards Regulations	6 months
Disclosure & Barring Service checks	Single Central Record Requirements under • for independent schools, (including academies and free schools and alternative provision academies and free schools): Part 4 of the	Record only satisfactory / unsatisfactory result and delete other information. If copy is kept, not to be retained beyond 6 months. See further DfE statutory Guidance ' Working Together to safeguard children' https://www.gov.uk/government/publications/working-together-to-safeguard-children--2

	Schedule to the Education (Independent School Standards) Regulations 2014; • for colleges: Regulations 20-25 and the Schedule to the Further Education (Providers of Education) (England) Regulations 2006;46 and	
Volunteer records		6 years from end of engagement
INSURANCE		
Employer's Liability Insurance	Employers' Liability (Compulsory Insurance Regulation) 1998	40 years
Policies	Commercial	3 years after lapse
Claims correspondence	Commercial	3 years after settlement
HEALTH & SAFETY / MEDICAL		
General records	Limitation Act 1970	Minimum 3 years
Records re work with hazardous substances	Control of Hazardous Substances to Health Regulations 2002	40 years
Accident books / records and reports	Reporting of Injuries Diseases and Dangerous Occurrences Regulations 1995	3 years after last entry or end of investigation
Medical Scheme documentation	Commercial	Permanent unless personal data is included
PREMISES / PROPERTY		
Original title deeds		Permanent / to disposal of property
Leases	Limitation Act 1980	12 years after lease has expired
Building records, plans, consents and certification and	Limitations Act 1980	6 years after disposal or permanent if of historical / archival interest.

warranties etc		
PENSION RECORDS		
Records about employees and workers	For all categories see: Detailed Guidance for Employers: (April 2017) pensions regulator.gov.uk	6 years
Records re the Scheme		6 years
Records re active members and opt in / opt out		6 years
PUPILS		
Educational Record	Pupil information Regulations 2005 (maintained schools only) Same approach applied in academy context. Data Protection regulation	25 years from date of birth unless passed to new school
Child Protection information (on child's file)	"Keeping children safe in education Statutory guidance for schools and colleges - September 2016"; "Working together to safeguard children. A guide to inter-agency working to safeguard and promote the welfare of children - February 2017"	RETAIN UNTIL FURTHER RECOMMENDATIONS Subject to moratorium on destruction due to historic child abuse enquiry. See https://www.iicsa.org.uk/document/guidance-note-retention-instructions-and-data-protection-requirements
Child Protection Information in other files	"Keeping children safe in education Statutory guidance for schools and colleges - September 2016"; "Working together to safeguard children. A guide to inter-agency working to safeguard and promote the welfare of children - February 2017"	RETAIN UNTIL FURTHER RECOMMENDATIONS Subject to moratorium on destruction due to historic child abuse enquiry. See https://www.iicsa.org.uk/document/guidance-note-retention-instructions-and-data-protection-requirements
Special Educational needs		

SEN files	Limitation Act 1980	Usually 25 years from date of birth of the pupil. If kept longer show good justification.
Education Health and Care Plans	Special Educational Needs and Disability Regulations 2014 Children and families Act 2014, part 3	25 years from date of birth of the pupil
Statements of Special Educational Needs (now historic)	Originally under Special Educational Needs and Disability Regulations 2001	25 years from date of birth of pupil unless passed to new school (usually on the pupil's file)
Attendance registers	Pupil Registration Regulations 2006 Regulation 14	3 years from when the register entry was made if made in paper registers For computerised registers retain until 3 years after the end of the school year during which the entry was made. Note: The difference in retention periods as between manual and computerised registers has probably come about in error but this is what the Regulations say.
Other items e.g. curriculum related, photographs, video recordings	Case by case basis	Look at why you are processing this and how long you need it for. Make sure you have a good justification for keeping it as long as you do. Set out the items and the justification.
PARENTS	Pupil Registration Regulations 2006 For basic name and contact details. Otherwise usually operational in accordance with the statutory functions of the school	Usually, for the duration that the parent has a pupil at the school. Otherwise subject to case by case justification.
ALUMNI AND THEIR PARENTS	Data protection regulation	For as long as there is an active relationship.