HATTON
ACADEMIES TRUST

Data Protection Policy

incorporating:

Freedom of Information & Subject Access Requests

School Records Management & Retention

Contents

1. Aims

Hatton Academies Trust aims to ensure that every item of personal data collected relating to staff, pupils, parents, directors, visitors and other individuals is collected, stored and processed in accordance with the UK Data Protection Law.

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:

- UK General Protection Data 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 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 within Trust Academies.

It also reflects the ICO's code of practice for the use of surveillance cameras on Trust premises and personal information for safeguarding and security purposes.

In addition, this policy complies with our funding agreement (at both Trust and individual Academy level) and the Trust's articles of association.

3. 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, holding, 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

The Trust and its constituent academies process personal data relating to parents, pupils, staff, directors, visitors and others, and therefore is a data controller.

The Trust 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 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 Trust Board of Directors (i.e. the Governing Board)

The Trust Board of Directors has overall responsibility for ensuring that the Trust and its constituent academies comply with all relevant data protection obligations.

5.2 Data Protection Officer

The Trust Data Protection Officer (DPO) is responsible for overseeing the implementation of this policy, monitoring Trust and individual Academy compliance with Data Protection Law, developing related policies and guidelines where applicable and providing support and advice to Academy Principals/Leaders with their data protection obligations, and ensuring that each academy has one officer trained in data protection compliance.

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

The DPO is also the first point of contact for individuals whose data the school processes, and for the ICO.

Full details of the DPO's responsibilities are set out in their job description (see **Appendix 2**).

The Trust DPO is Colin Hinds and is contactable as follows:

Via e-mail: dataprotectionofficer@hattonacademiestrust.org.uk

Via telephone: 01933 231271

Via post: Orchard House, 79 Gold Street, Wellingborough, NN8 4EQ

5.3 Academy Principal

The Principal of each Academy acts as the representative of the data controller on a day-to-day basis with responsibility for ensuring that the Academy is operationally compliant with this policy and for ensuring that Academy staff receive regular training and guidance on their data protection obligations.

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
- Conducting Data Protection Impact Assessments (DPIAs) when new information systems and processes (digital or paper based) are implemented, or where existing information systems and processes are updated or changed (see **Appendix 3**).
- 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 (no matter how minor) and including near misses (e.g. loss of control of personal data which could have resulted in a breach)
- Whenever they are engaging in a new activity that may affect the privacy rights of individuals
- For support and advice on Data Protection Impact Assessments (DPIAs)
- If they need help and advice with the data protection terms and conditions of contracts or sharing personal data with third parties
- Co-operating with investigations in the event of a potential or actual data breach

6. Data Protection Principles

The UK GDPR is based on 6 data protection principles that the 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 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 pupil) has freely given clear **consent**.

The pupil's consent statement will override any previous consent statement of the parent/carer in all cases, provided that the child has the capacity to understand the implications of the consent decision. Where parents have concerns about their child's consent decision, they should discuss this with their child or, in cases where they are concerned that their child does not have the capacity to make a consent decision, they should discuss this with the Academy Principal.

7.2 Special Categories of Personal Data
For special categories of personal data, defined on page 6, we will also meet one of the following special category conditions for processing under data protection law:

- The individual (or their parent/carer when appropriate in the case of a pupil) has given **explicit consent**
- The data needs to be processed to perform or exercise obligations or rights in relation to **employment, social security or social 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 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.

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

7.3 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.

When staff no longer need the personal data they hold, they must ensure it is deleted, destroyed or anonymised. This will be done in accordance with the Trust's records retention and management procedures. **See Appendix 6.**

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, which includes a data sharing 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 or staff.

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

In all circumstances where personal data is lawfully shared with any third party (including parents, directors and staff) the following protocols must be followed:

- **Sharing digital personal data** - all digital personal data must only be sent to a third party, staff member, director, parent, using an encrypted email, sent from the Trust email servers. See **Appendix 5** for detailed instructions on sending encrypted emails using Office 365.

- **Sharing paper based personal data** – all paper based personal data must be delivered to the recipient securely. Where postal services are used for delivery, staff should ensure that the envelope/package is signed for by the recipient only.

  Alternatively paper based personal data can be delivered by hand to the recipient only. Where required staff should take appropriate measures to validate the true identity of the recipient.

9. Statutory Information 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 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 isn't 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 must be submitted in any form to the DPO, but we will 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 they must immediately forward it to the DPO to ensure that the statutory response times can be met.

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 for the parents or carers to receive this information.

Children below the age of 13 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 Trust Primary Academies may be granted without the express permission of the pupil. This is not a rule and a pupil's ability to understand their rights will always be judged on a case-by-case basis.

Children aged 13 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 at Trust Secondary Academies may not be granted without the express permission of the pupil. This is not a rule and a pupil's ability to understand their rights will always be judged on a case-by-case basis.

9.3 Responding to Subject Access Requests

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). For example a request received on 1st August must be responded to by 1st September.
- 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 cannot reasonably anonymise, and we do not have the other person's consent without which it would be unreasonable to proceed
- 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
- Is restricted by the stipulations within adoption or parental order records
- Is given to a court in proceedings concerning the child.

In all cases, the impact on the child and their wellbeing will be assessed before a response to a subject access request is released.

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 in nature, 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 or they can seek to enforce their subject access right through the courts.

9.4 Freedom of Information Act Requests
As a public authority the Trust is required by law to respond to requests for information to be provided under the Freedom of Information Act 2000 (FOIA). All FOIA requests must be dealt with by the DPO in accordance with statutory timescales and therefore it is essential that staff receiving such requests directly forward these to the DPO at the earliest opportunity.

Full details of the Trust FOIA guidelines are attached to this policy at **Appendix 4**.

9.5 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
- 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.

10. Parental Requests to see the Educational Record

Parents, or those with parental responsibility, will be granted free access to their child's educational record on request (which includes most information held about a pupil) within 15 school days of receipt of a written request.

Parents should note that for children aged 13 or older, the consent of the child will also be sought and must be received prior to release of the educational record.

The Trust will not charge parents any fee to access this information and may be asked if they wish to either:

a) view the educational record in person on the school or

b) receive a copy of the educational record by e-mail

Requests should be made in writing to the Principal of the Academy.

11. Biometric Recognition Systems

Where we use pupils' biometric data as part of an automated biometric recognition system (for example, pupils use finger prints to loan library books, 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 (or from the child where they are in Year 8 or above) before we take any biometric data from their child and first process it.

Parents/carers and pupils 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 pupils. Parents/carers and pupils can object to participation in the school's 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 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 their parents/carers.

12. CCTV

We use CCTV in various locations around the school site to ensure it remains safe. We will adhere to the ICO's guidance 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 Principal of the relevant academy. If following such enquiries data protection concerns still exist, then these should be escalated to the DPO.

13. Photographs and Videos

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

In our Primary Academies, 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.

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

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

Uses may include:

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

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 and training 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 school's processing of personal data presents a high risk to rights and freedoms of individuals, and when introducing new technologies (the DPO will advise staff 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 to ensure compliance with, and understanding of, this policy
- 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, any transfers of personal data outside of the UK and the safeguards in place for those, 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 or sharing.

In particular:

- Where data is shared digitally, email encryption must be used in all instances, see **Appendix 5.**
- Where paper based records are shared, secure delivery will be used in all instances
- Paper-based records should be kept under lock and key when not in use
- Computers and portable electronic devices, such as laptops, iPads, tablets and mobile phones that are used to access personal data will be protected by secure password or passcode
- All laptops and PC's will be protected by password protected screensavers activated when staff are away from their workstations
- 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, prior approval from the Academy Principal should be obtained and staff must sign all records in and out
- All digital personal data will be stored on Trust servers accessed by secure login
- All passwords used on to access Trust IT equipment and software must be in line with the Trust Password Policy
- The Trust has prohibited the use of removable media for the storage of data (eg. usb devices, external hard drives, cd/dvd roms). Where data is received from other organisations on a removable device (e.g. exam boards and photos of educational activities), the device should be approved as cyber secure prior to use.
- Staff, pupils or directors who store personal information on their personal devices are expected to follow the same security procedures as for school-owned equipment. See Trust Online Safety 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

The school 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, the Data Protection Officer will report the data breach to the ICO within 72 hours after becoming aware of it. **All communications with the Information Commissioners Office must be made by the Data Protection Officer**.

Such breaches in a school context may include, but are not limited to:

- A non-anonymised dataset containing personal data relating to pupils being emailed to multiple parents
- 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/usb storage device containing non-encrypted personal data about pupils or staff
- A cyber security breach.

18. Training

All staff (including volunteers) 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 Trust processes make it necessary.

19. Monitoring Arrangements

The DPO is responsible for monitoring and reviewing this policy.

This policy will be reviewed annually and approved by the Board of Directors.

20. Links to other Policies

This Data Protection Policy is linked to our:

- Online Safety Policy (inc. Acceptable use Agreement)
- Child Protection Policy
- Digital Photographs & Images Policy
- Password Policy

Appendix 1. Personal Data Breach Procedure

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, director or data processor must immediately notify the data protection officer (DPO) by email to dataprotectionofficer@hattonacademiestrust.org.uk
- 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 and directors must 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 CEO in all circumstances and the Chair of the Board of Directors where breaches are deemed notifiable to the ICO.
- 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 system providers). See the actions relevant to specific data types 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) before and after the implementation of steps to mitigate the consequences
- The DPO will determine 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 school'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 school'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 school 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)

Records of all breaches will be recorded digitally within the Trust secure folders.

The DPO will review what happened and how it can be stopped from happening again and liaise with appropriate leaders/managers to determine remedial actions.

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.

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, the DPO will ask IT Services to attempt to recall it on their behalf 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 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 school should inform any, or all, of its 3 local safeguarding partners
- A risk assessment will be carried out by the DPO to establish the impact on the data subject rights and freedoms.

Appendix 2. Trust Data Protection Officer - Role Description

Purpose

The DPO is responsible for monitoring compliance with current data protection law, and has the knowledge, support and authority to do so effectively. They oversee the Trust's data protection processes and advise the Trust and its academies on best practice.

Key Responsibilities

To:

- Advise the Trust Academies and its employees about their obligations under current data protection law, including the General Data Protection Regulation (GDPR)
- Develop an in-depth understanding of the Trust's processing operations, information systems, data security processes and needs, and administrative rules and procedures
- Monitor the Trust Academies compliance with data protection law, by:
    - Collecting information to identify data processing activities
    - Analysing and checking the compliance of data processing activities
    - Informing, advising and issuing recommendations to Trust academies
    - Ensuring they remain an expert in data protection issues and changes to the law, attending relevant training as appropriate
- Ensure the Trust's policies are followed, through:
    - Assigning responsibilities to individuals
    - Awareness-raising activities
    - Co-ordinating staff training
    - Conducting internal data protection audits
- Advise on and assist the Trust academies with carrying out data protection impact assessments, as required.
- Act as a contact point for the Information Commissioner's Office (ICO), assisting and consulting it where necessary, including:
    - Helping the ICO to access documents and information
    - Seeking advice on data protection issues
- Act as a contact point for individuals whose data is processed (for example, staff, pupils and parents), including:
    - Responding to subject access requests
    - Responding to other requests regarding individuals' rights over their data and how it is used
- Take a risk-based approach to data protection, including:
    - Prioritising the higher-risk areas of data protection and focusing mostly on these
    - Advising the academies if/when they should conduct an internal data protection audit, which areas staff need training in, and what the DPO role should involve
- Report to the Board of Directors on the Trust Academies' data protection compliance and associated risks

- Respect and uphold confidentiality, as appropriate and in line with data protection law, in carrying out all duties of the role
- Support Academy Principals and Managers to maintain a record of the academy's data processing activities
- Work with external stakeholders, such as suppliers or members of the community, on data protection issues
- Take responsibility for fostering a culture of data protection throughout the Trust
- Work closely with other departments and services to ensure GDPR compliance, such as HR, Legal, IT Services, Finance and Premises / Security

It is recommended that the DPO must:

- Be a senior member of staff, reporting directly to the Board of Directors
- Have a role which is compatible with the DPO role, in terms of time and workload
- Not have any conflicts of interest between their current role and the DPO role

Appendix 3. Data Privacy Impact Assessments (DPIA)

Guide to completing a DPIA

A DPIA is a process which helps an organisation to identify and reduce the privacy risks to individuals whose personal information is used in a project. The Data Protection Act will make it a legal requirement to carry out a DPIA where the use of the personal information is likely to result in a **high** risk to the privacy of individuals.

Examples might include use of new technologies, including proposals to use cloud storage facilities for school information, use of software that uses details from the SIMS database, use of CCTV and biometrics, such as finger print scanning.

A DPIA can be used to help you to design more efficient and effective ways for handling personal data, minimise privacy risks to the individuals affected and financial and reputational impact of a data incident on the school.

This guide is intended to help you assess whether a DPIA is needed, identify levels of risk of personal data for your project and complete a DPIA report (where applicable), which will need to be agreed and approved by the Data Protection Officer.

When to carry out a DPIA

A DPIA should be completed when the project is likely to involve collection of personal data that may involve a high risk to the privacy of individuals. You should take into account the following when deciding whether a DPIA is necessary.

1. If personal data is not being collected or processed there is no need to do a DPIA.

2. Will the project involve the collection of new or different types of information about individuals? If personal information will be collected using new technology, or collection of a new type of special category data not collected before, you should carry out a DPIA. If you will be collecting large amounts of personal information to use in a way not previously used, you should complete a DPIA.

3. Any project involving monitoring of individuals, such as installation of new CCTV, should always require a DPIA as should any use of biometric technology.

When to start a DPIA

If you are thinking about starting a project or making changes to existing services/systems, then you should consider whether a DPIA is necessary from an early stage.

A DPIA should be started at project initiation stage, continued throughout the life of the project and re-visited in each new project phase, for example, when you want to use the personal data for a new or additional purpose for the use of the data, or if you are collecting new personal data. This should be proportionate to the level of special category data being collected or processed as a result of the project.

It is important to start at an early stage of the process to allow for time to resolve issues and mitigate for any risks identified, in order to avoid the difficulties of having to address these points late in the project when other decisions have already been made.

How to carry out a DPIA

Use the checklist below to help you decide whether the project involves privacy risks, identify what they are and work out what steps you will need to take to minimise those risks as far as possible.

When you have considered all of the risks, you should come to a conclusion about anything you can do to eliminate or minimise the risks you have identified. Some examples might include:-

- Minimising the risks of collecting too much personal information on CCTV by siting and angling the cameras so that they are focussed only on perhaps the car park rather than the entire school playground, or the entrance door, not into the school office.
- Checking the questions you have asked on a form before you send it out and ensuring that you really need all of the personal information you have requested
- If you need to store personal information on paper records ensuring that you keep them in a secure location which cannot be readily accessed by unauthorised individuals.
- If using a laptop in a classroom, make sure that staff are instructed to lock the screen if they leave it unattended for a while.

When you have recorded all of these points and how you will address the risks, you should get it signed off – either by the Data Protection Officer (or if the Data Protection Officer is completing the form, by the CEO) and keep a copy to refer back to for audit purposes and for updating if the project is changed or extended in future.

Completing a DPIA

A Microsoft Form has been created for the purpose of completing DPIA's for the Trust. When you have completed the online DPIA, considered any risks and mitigated them wherever possible, please submit the form and the Trust will then review the details and decide whether to accept any remaining risks. It is good practice to document what risks were identified, what steps were taken to minimise them and what risks were accepted.

The Data Protection Officer, DPO, will sign off the final DPIA and confirm to you if this has been approved.

You can find more detailed guidance on conducting privacy impact assessments on the ICO's DPIA code of practice

https://ico.org.uk/media/about-the-ico/consultations/2052/draft-conducting-privacy-impact-assessments-code-of-practice.pdf

DPIA Checklist

- What is the software/application for? What does it seek to achieve?
- Will the project collect information about individuals, e.g. students, parents, staff?
- What personal information will it collect? Please list. (i.e. Name, D.O.B.)
- Will it be special category data? e.g. information about an individuals physical or mental health, social care details, details of criminal offences or allegations, or collecting large quantities of personal information? Any of these will raise the level of risk.
- How will the information be collected?
- Who will have access to this information outside of the provider's organisation?
- How will it be stored and kept secure by the provider?
- How will pupils/staff/parents be made aware of how their personal information is being used?
- Does the school privacy notice provide sufficient detail about the reasons for collecting the information and who it may be shared with?
- Do you need consent from the individual to use the information? e.g. because special category data is being collected.
- Does the project involve the use of new or different technology which could be privacy intrusive e.g. CCTV, monitoring of staff, biometrics, GPS tracking or cloud storage
- What risks have been identified? What steps have been taken to eliminate or minimise them?
- Does the platform support Multi-Factor Authentication (MFA)?
- Who will be the administrators for the software/platform?

Appendix 4. Freedom of Information Requests

Introduction

The Board of Directors of Hatton Academies Trust takes its statutory responsibilities under the Freedom of Information Act 2000 seriously. All academies within the Trust are committed to the principles of public accountability and the general right of access to information, subject to the appropriate legal exemptions. This publication scheme outlines the Trust's designated framework for managing requests.

Under the Freedom of Information Act 2000 (herein referred to as 'FOIA'), every person has a legal right to request information held by the academies, which is deemed to be information held by a public authority. Those making requests are entitled to be informed whether the Trust holds the information requested, and subject to certain exemptions, to be furnished with a copy within prescribed deadlines.

The information which the trust routinely makes available to the public includes information available on the academies' website and Virtual Learning Environments. Requests for other information are dealt with in accordance with statutory guidance. Whilst the FOIA assumes openness and transparency with public requests for information, it recognises that certain information is by its very nature sensitive. There are exemptions to protect this information, which may result in a request for information being denied.

The Act is fully retrospective, so that any past records which the academy holds is covered by the Act. All academies within the trust hold a Records Retention Schedule based on the schedule recommended by the Records Management Society of Great Britain, which guides the academy as to how long it should keep records. The Trust recognises that it is an offense under FOIA to wilfully conceal, damage or destroy information in order to avoid responding to an enquiry, so it is important that no records that are the subject of an enquiry are amended or destroyed.

Requests under the Act can be addressed to anyone employed by the academy. However, all responses are to be cleared by the Trust's Data Protection and Freedom of Information lead, the Director of Finance and Operations, or the Executive Principal prior to information being released.

The Trust will ensure that staff in every Academy are fully aware of the process for dealing with requests. Requests must be made in writing, (which can include email), and should include the enquirers name and correspondence address, and state what information they require.

They do not have to mention the FOIA, nor do they have to say why they want the information. The Trust recognises its duty to respond to all requests, advising the person

or organisation requesting the information swiftly whether or not the information is held, and supplying any information that is held, except where exemptions apply. There is a statutory time limit of 20 working days for responding to the request. In accordance with the ICO guidelines, a working day means any other day than a Saturday, Sunday or UK Bank Holiday. School holiday periods are therefore counted as working days under the Freedom of Information Act.

2. Scope

The Director of Finance and Operations is responsible for ensuring compliance with Academy Policies and Procedures. This procedure applies to all staff employed by Hatton Academies Trust.

Requests for personal data are still covered by the Data Protection Act. Individuals can request to see what information the Academy holds about them. This is known as a Subject Access Request, and must be dealt with in accordance with the Trust's Data Protection Policy.

3. Procedure

3.1 The Trust's Statutory Duty

The Trust Board of Directors recognises its statutory duty to advise and assist anyone requesting information from an academy within the trust. In this respect, the trust will respond to straightforward verbal requests for information and will help enquirers to put more complex verbal requests into writing so that they can be handled under the Act.

The Board of Directors recognises the duty to:

a) confirm to those making requests whether or not the Trust holds the information requested (known as 'the duty to confirm or deny'), and

b) provide access to the information we hold in accordance with our procedures

3.2 Publication Scheme

The Trust has a written Publication Scheme derived from the Model Publication Scheme for Schools approved by the Information Commissioner. The Publication Scheme is available from the Trust on request.

3.3 Responding to FOIA Requests
The trust will respond to all requests in accordance with the Freedom of Information Act provisions. Responses will be in writing only.

3.4 Exemptions
Certain information is subject to certain exemptions. Persons requesting information under FOIA will be advised if an exemption applies.

When we wish to apply a qualified exemption to a request, we will invoke the public interest test procedures to determine if public interest in applying the exemption outweighs the public interest in disclosing the information.

We will maintain a register of requests where we have refused to supply information, and the reasons for the refusal. The register will be retained for 5 years from the date of the request.

3.5 Public Interest Test
Unless it is in the public interest to withhold information, it has to be released. We will apply the Public Interest Test before any qualified exemptions are applied.

3.6 Charging
We reserve the right to refuse to supply information where the cost of doing so exceeds the statutory maximum, currently £450.

The Board of Directors reserves the right to charge a fee for complying with requests for information under FoIA. The fees are calculated according to FoIA regulations, and the person notified of the charge before the information is supplied.

4. Responsibilities

The Board of Directors has delegated to the day-to-day responsibility for compliance with the FoIA to the Director of Finance and Operations. A member of staff will be nominated to co-ordinate enquiries and to be a point of reference for advice and training.

5. Complaints

Any comments or complaints will be dealt with through the Academy Trust's normal complaints procedure.

If, on investigation, the Academy's original decision is upheld, then the Academy has a duty to inform the complainant of their right to appeal to the Information Commissioner's Office.

Appeals should be made in writing to the Information Commissioner's Office at: FOI/EIR Complaints Resolution Information Commissioner's Office
Wycliffe House, Water Lane
Wilmslow, Cheshire SK9 5AF

Appendix 5. Encrypting Documents and Emails

Protect a document with a password - Microsoft Support

Protect a document with a password

Word for Microsoft 365, Word for Microsoft 365 for Mac, Word for the web, Word 2021, More...

Passwords are case-sensitive and can be a maximum of 15 characters long.

If you lose or forget your password, Word won't be able to recover it for you. Be sure to keep the a copy of the password in a safe place or create a strong password that you'll remember.

Windows macOS - newer Word for Mac 2011 Web

1. Go to **File** > **Info** > **Protect Document** > **Encrypt with Password**.
2. Type a password, then type it again to confirm it.
3. Save the file to make sure the password takes effect.

Protect an Excel file - Microsoft Support

Protect an Excel file

Excel for Microsoft 365, Excel for Microsoft 365 for Mac, Excel 2021, Excel 2021 for Mac, More...

To prevent others from accessing data in your Excel files, protect your Excel file with a password.

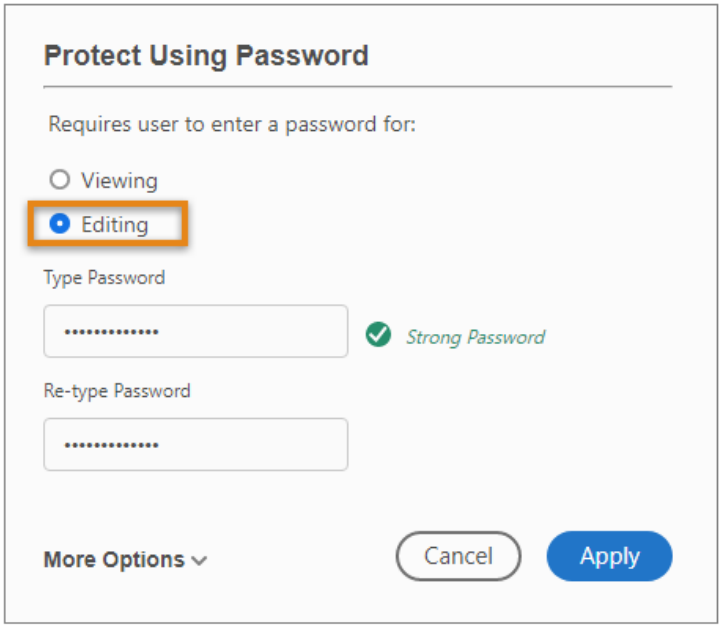
1. Select **File** > **Info**.
2. Select the **Protect Workbook** box and choose **Encrypt with Password.**
3. Enter a password in the **Password** box, and then select **OK**.
4. Confirm the password in the **Reenter Password** box, and then select **OK**.

Adobe [Securing PDFs with passwords, Adobe Acrobat]

Restrict editing of a PDF

You can prevent users from changing PDFs. The restrict editing option prohibits users from editing text, moving objects, or adding form fields. Users can still fill in form fields, sign, or add comments.

1. Open the PDF in Acrobat, and do one of the following:
   - Choose **File** > **Protect Using Password**.
   - Choose **Tools** > **Protect** > **Protect Using Password**.
2. If you receive a prompt, click **Yes** to change the security.
3. Choose **Editing**, and then type and retype your password. Your password must be at least six characters long. The password strength is displayed next to your password to indicate whether the chosen password is weak, medium, or strong.



[Encrypt an Email in Outlook]

Office365 has built-in email encryption:

1. When you create an email, please ensure that in the Subject Line you include the word Confidential – this will automatically encrypt the email you are sending.
2. The email recipient will be redirected to Microsoft 365 and prompted to either sign in to their account or sign in with a passcode, which will then be emailed to them.

Appendix 6. Information & Records Management Retention Guidelines

The Academy recognises that, by efficiently managing its records, it will be able to comply with its legal and regulatory obligations and to contribute to the effective overall management of the institution. Records provide evidence for protecting the legal rights and interests of the Academy, and provide evidence for demonstrating performance and accountability.

This document provides the framework through which this effective management can be achieved and audited. It covers:

- Scope
- Responsibilities

Scope

- These guidelines applies to all records created, received or maintained by permanent and temporary staff of the Academy in the course of carrying out its functions. Also, by any agents, contractors, consultants or third parties acting on behalf of the Academy.
- Records are defined as all those documents which facilitate the business carried out by the Academy and which are thereafter retained (for a set period) to provide evidence of its transactions or activities. These records may be created, received or maintained in hard copy or electronic format, e.g., paper documents, scanned documents, e-mails which document business activities and decisions, audio and video recordings, text messages, notes of telephone and Skype conversations, spreadsheets, MS Word documents, and presentations.

Responsibilities

- The governing body of an Academy has a statutory responsibility to maintain the Academy records and recordkeeping systems in accordance with the regulatory environment specific to the Academy. The responsibility is usually delegated to the Head Teacher of the Academy.
- The person responsible for day-to-day operational management in the Academy will give guidance on good records management practice and will promote compliance with this policy, so that information will be retrieved easily, appropriately and in a timely way. They will also monitor compliance with this policy by surveying at least annually to check if records are stored securely and can be accessed appropriately.
- The Academy will manage and document its records disposal process in line with the Records Retention Schedule and evidence this in the form of a Records Disposal Log. This will help to ensure that it can meet FOI requests and respond to requests to access personal data under data protection legislation (subject access requests, SARS).
- Individual staff and employees must ensure, with respect to records for which they are responsible, that they:
    - Manage the Academy's records consistently, in accordance with the Academy's policies and procedures
    - Properly document their actions and decisions
    - Hold personal information securely

- Only share personal information appropriately and do not disclose it to any unauthorised third party
- Dispose of records securely, in accordance with the Academy's Records Retention Schedule

For detailed guidance on retention and disposal timescales for all information held within the Trust and its academies, please refer to the **HAT Information and Records Management Retention Guidance** on the Data Protection page of the Trust Website.