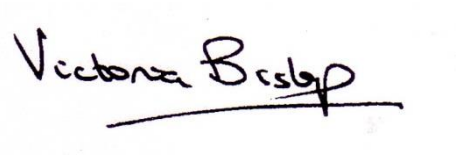
Hatton Academies Trust

Title	**HAT Data Protection Policy**
Reviewed	**September 2018**
Next Review	**September 2019**
Associated Policies	**Freedom of information publication scheme** **E-safety policy** **Confidentiality Policy** **Child Protection Policy** **Employee Code of Conduct**
Originator	**Colin Hinds**
Approved	

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 General Data Protection Regulation (GDPR) and the expected provisions of the Data Protection Act 2018 (DPA 2018).

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 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 within Trust Academies.

It also reflects the ICO's code of practice for the use of surveillance cameras 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 and its academies are 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

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) has delegated responsibility from the Board of Directors 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 ensuring that staff receive training on their data protection obligations.

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: Sir Christopher Hatton Academy, The Pyghtle, Wellingborough, NN8 4RP

5.3 Academy Principal / Head of School

The Principal / Head of School 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.

5.4 All Staff

Staff are responsible for:

- Collecting, storing and processing any personal data in accordance with this policy
- Informing their Academy of any changes to their personal data held by the Academy, 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 (no matter how minor)
    - 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 any contracts or sharing personal data with third parties

6. Data Protection Principles

The GDPR is based on 6 data protection principles that all academies 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 and its constituent academies aim 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 school can **fulfil a contract** with the individual, or the individual has asked the school to take specific steps before entering into a contract
- The data needs to be processed so that the school can **comply with a legal obligation**
- The data needs to be processed to ensure the **vital interests** of the individual e.g. to protect someone's life
- The data needs to be processed so that the school, 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 the school 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**.

It should be noted that the age of consent for Data Protection matters is 12 years old in the UK and therefore, **secondary school pupils in Year 8 and above will be asked to provide their own consent** where required (e.g. for photographic images, biometric data etc).

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 / Head of School.

For special categories of personal data, as well as meeting one of the above, we will also meet one of the special category conditions for processing which are set out in Article 9 of the GDPR and Data Protection Act 2018, as listed on page 2 of this policy.

In Trust Primary Academies which offer online services to pupils, 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).

In Trust secondary schools which offer online services to pupils, such as classroom apps, and we intend to rely on consent as a basis for processing, we will get parental consent where the pupil is in Year 7 (except for online counselling and preventive services). Pupils in years 8 and above will determine whether they consent to these processing activities.

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, destroyed or anonymised. This will be done in accordance with the school's 'records retention and management' policy, which is based on the Information and Records Management Society's toolkit for schools.

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 or parent/carer that puts the safety of our staff at risk
- There is a medical emergency involving a pupil, staff member, director, volunteer, etc.
- 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 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 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 an Academy and/or 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
- 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, email or fax 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 for the parents to receive this information.

Children below the age of 12 are generally not regarded to be mature enough to understand their rights and the implications of a subject access request. Therefore, most subject access requests from parents or carers of pupils at Trust 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 12 and above are generally regarded to be mature enough to understand their rights and the implications of a subject access request. This understanding will be reinforced by the Academy in lifeskills lessons. 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. 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
- 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 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.

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, 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 over the age of 12, the consent of the child will also be sought.

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 or Head of School of the Academy. There will be no charge to parents for the provision of this information.

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 the pupil or their parent(s)/carer(s).

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 Principal / Head of School of the relevant academy.

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.

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 privacy 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 surveys, reviews and audits to test our privacy measures and to provide evidence of compliance 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, 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
- Password encryption is used to access school computers, laptops and other electronic devices. Staff and pupils 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 or directors who store personal information on their personal devices are expected to follow the same security procedures as for school-owned equipment
- 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, we will report the data breach to the ICO within 72 hours. Such breaches in a school context may include, but are not limited to:

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

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 the school's 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 our school's practice. Otherwise, or from then on, this policy will be reviewed **annually** and shared with the Board of Directors.

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 Principal / Head of School, CEO and Chairman of the results of the investigation.
- The DPO will make assemble a team of staff 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.

  If there is any doubt, then the DPO will contact the ICO to seek their advice.
- 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 in a central secure file held by the Data Protection Officer.
- Where the ICO must be notified, the DPO will do this via the 'report a breach' page of the ICO website as soon as possible, but in any case within 72 hours. 72 hours should be considered a longstop deadline and where possible, steps will be taken to ensure that a breach is reported within 24 hours of it being discovered. 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 in a central Trust register held by the Data Protection Officer.
- The DPO and Principal / Head of School 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 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 it's academies on best practice.

Key Responsibilities

To:

- Advise the Trust Academies and it's 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 Protection Guidance – Encrypting an External Storage Device

To comply with data protection regulations, **ALL** USB/Memory Sticks and all other external storage devices (including CDs, DVDs, and external hard drives) that are to be used in school need to be encrypted, where they contain personal data.

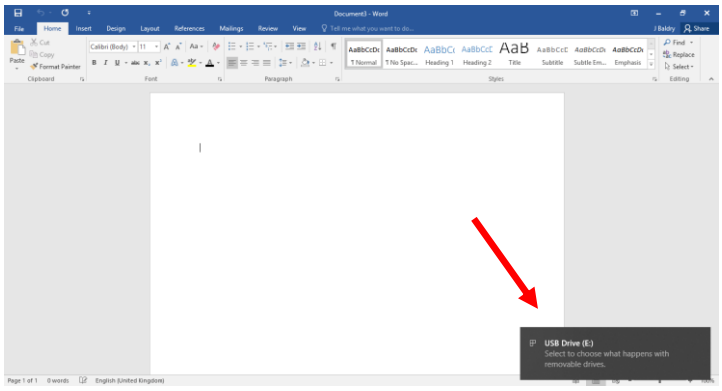
When encrypting a device, it is recommended that you start with a new or empty one or delete / backup any files that you no longer need from your stick as used devices containing files can take longer for encryption.

WARNING – Used USB stick encryption could take hours or even days to complete depending on the amount and size of files.

The following procedure should be followed to encrypt a storage device using Microsoft Windows Bit locker.

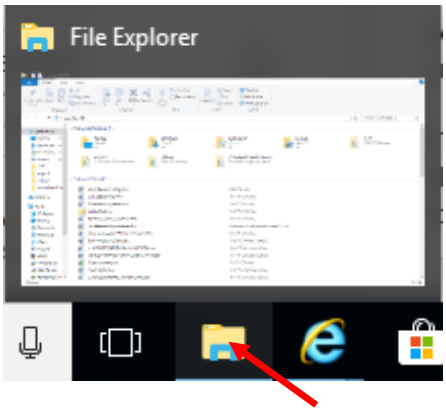
Step 1

- Insert your USB stick into the USB port on your pc or laptop and wait.
- Your PC will automatically set up the drive to be accessed. The letter of the USB drive will vary depending on the amount of normal drives in your machine.
- Wait for the drive to be appear. A pop up message should be shown once the drive is successfully installed. If no pop up message appears follow Step 2.

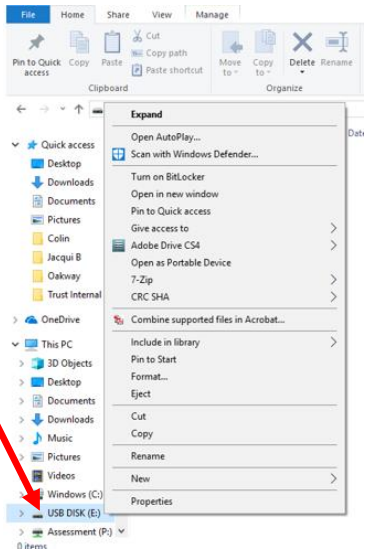


Step 2

- Click on File Explorer on your desktop.



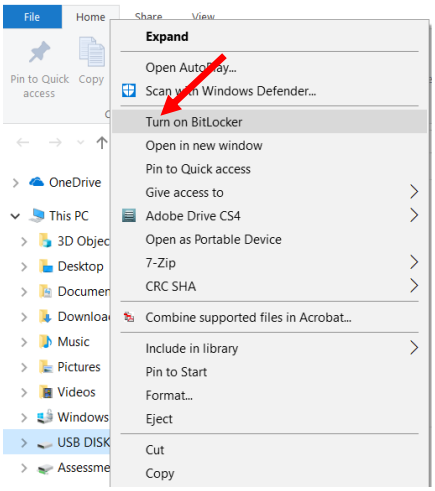
- Right click on USB drive.



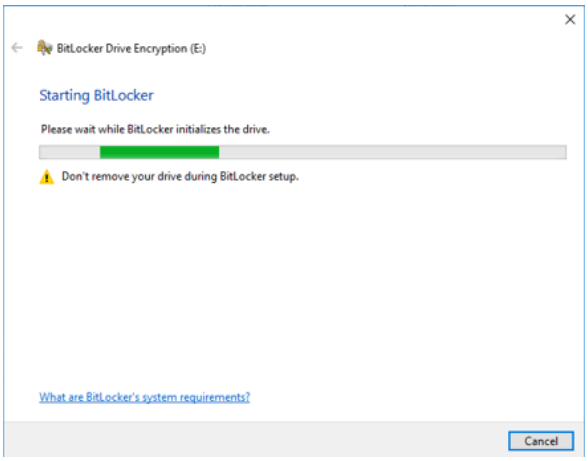
Step 3

Step 4

- Left click on Turn On BitLocker.

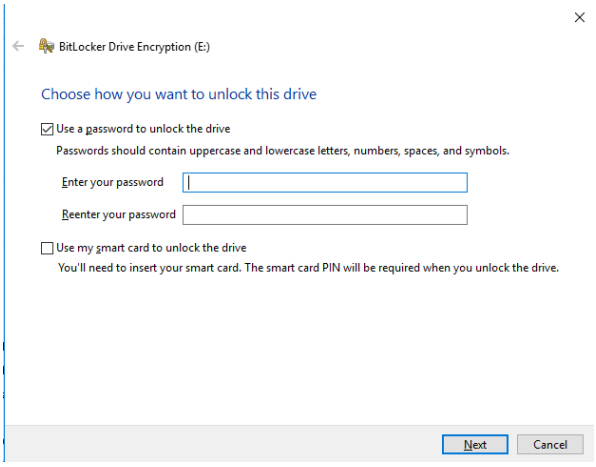


- BitLocker will automatically start Encrypting your USB Stick.



Step 5

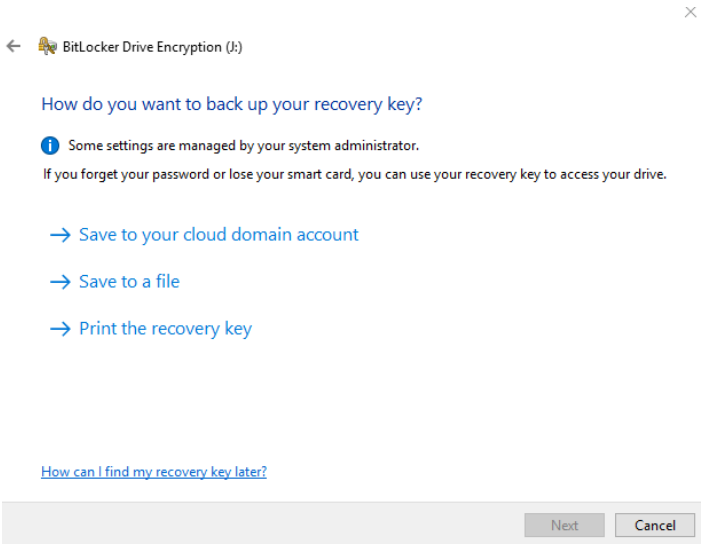
- BitLocker will ask how you would like to unlock your drive.
- Choose the option *Use a password to unlock the drive.*



- Enter the password you would like to use to unlock your USB stick.
- Click on Next.

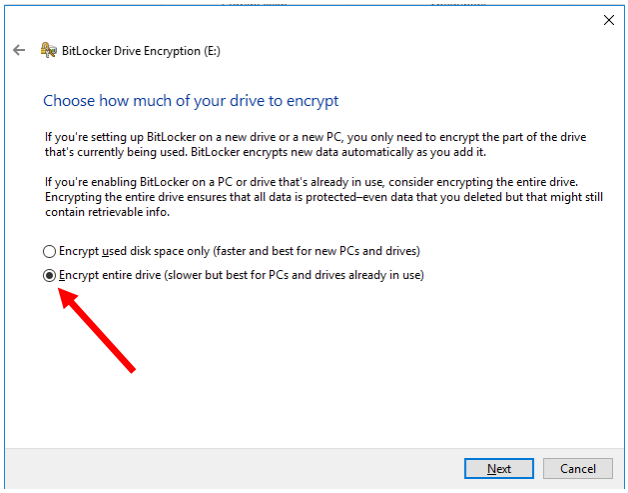
Step 6

- As your password is unique to you, IT services **will not** be able to decrypt if you lose the password.
- If you do lose your password you can set up a recovery key to access your drive. Select how you would to do this and then click Next.



Step 7

- Choose how much of your drive you would like to encrypt.



- It is recommended that you encrypt the entire drive if you already have files on your drive. (Be aware that this could take a long time to encrypt)

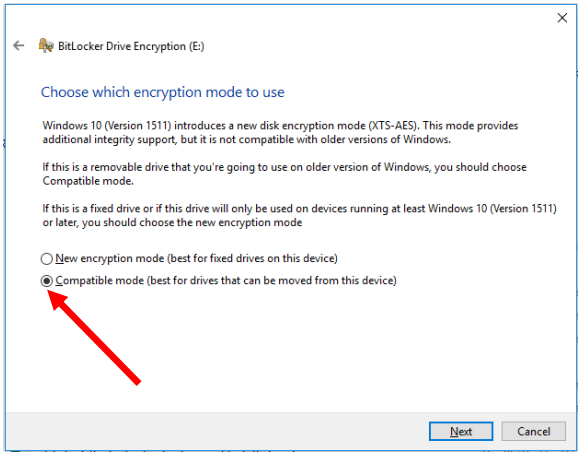
- If possible start the academic year with a brand new USB Stick.

- Click on Next.

Step 8

- Choose which encryption mode to use.

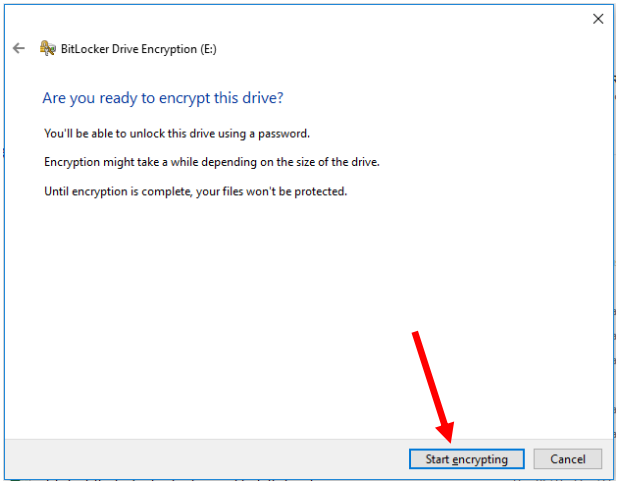
- Select *Compatible mode,* if you will use your USB stick in different machines. If you do not select this your USB stick may not be recognised on different machines.



- Click on Next.

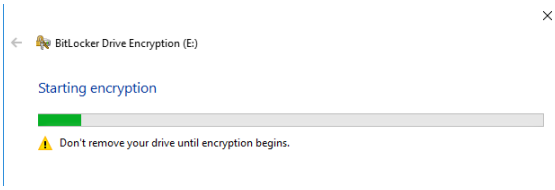
Step 9

- Click on *Start encrypting*



Step 10

- Encryption will begin.



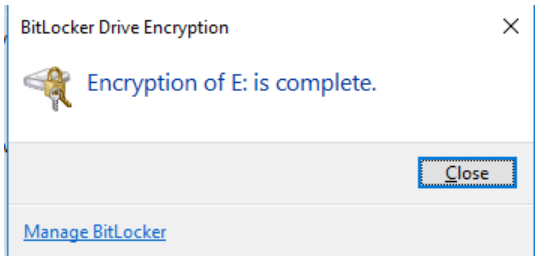
- As a guide a new unused USB stick can take approximately 5 to 15 minutes to encrypt.

- DO NOT REMOVE YOUR USB STICK UNTIL THIS PROCESS IS COMPLETE. If you do have to remove the USB stick before it is finished, please ensure that you pause the process before removing it, otherwise it may be unusable.

WARNING - If you already have files saved on your USB stick, encryption could take hours or even days to complete depending on the size.

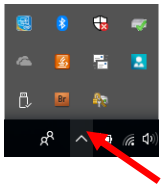
Step 11

- Once encryption is complete click on *Close.*

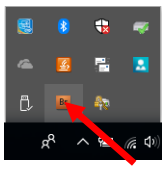


Step 12

- To safely remove your USB stick from the USB port click on the arrow on your desktop.



Next click on USB symbol

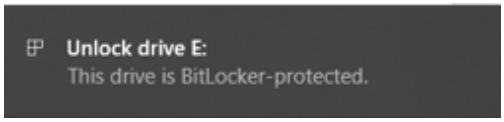


- Click on Eject Flash Disk

- Wait for the following message to appear and then remove your USB stick from the port.

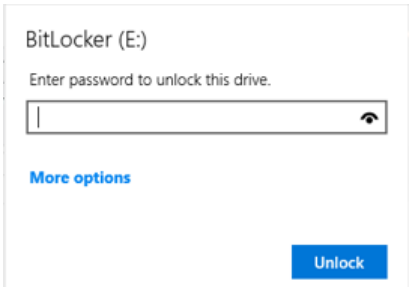
Step 13

- Each time that you use your encrypted USB stick you will get the following message appear when you plug it into the USB port.



Step 14

- Enter your password to enable your USB stick.

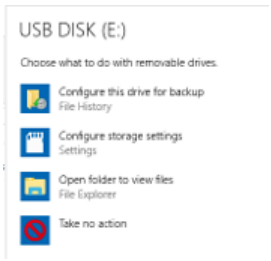


- Click on Unlock

Step 15

- You can then choose what to do with the drive.
- Continue working as usual.

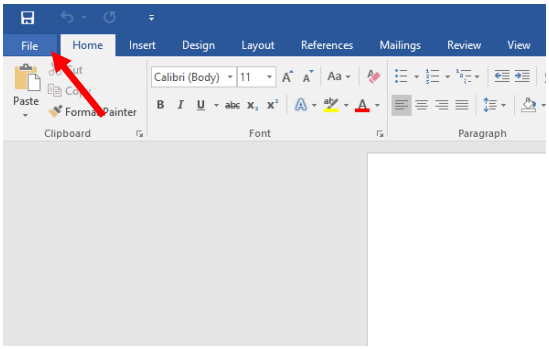
<u>Please Note:</u>

	It is essential that you back your files up to a network server on a regular basis to avoid loss of files if either your USB stick is misplaced or in the event of corruption.

Appendix 4 Encrypting a Word Document

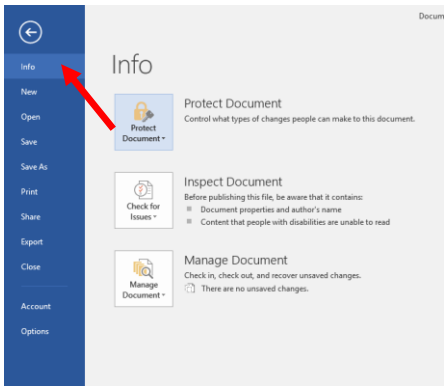
Step 1

- To Encrypt a word document that you have created click on File.



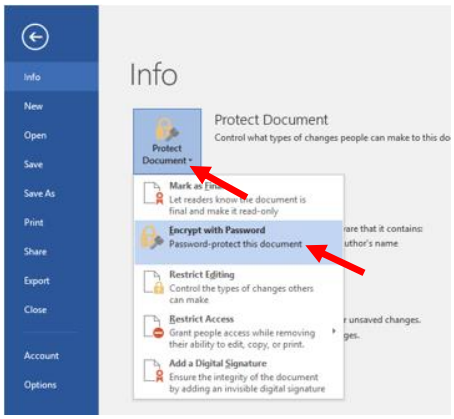
Step 2

- Click on Info.



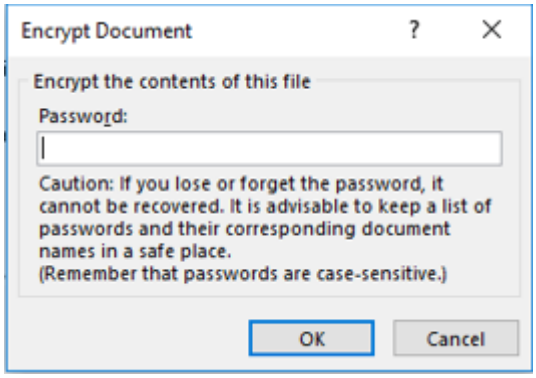
Step 3

- Click on the drop down arrow on Protect Document.
- Click on Encrypt with Password.



Step 4

- Enter the password you wish to use to open this document.



- Click on OK.

Step 5

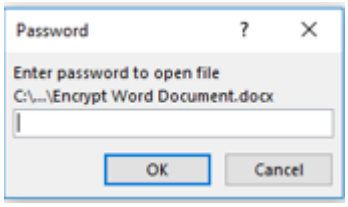
- Re enter password.

Step 6

- Your document is now protected and will require the password to be entered to open it.

- Click on OK.

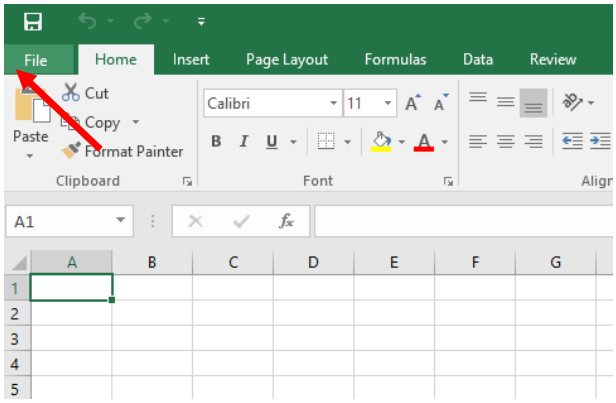
- Next time you open your protected document you will be prompted to enter the password.



Appendix 5. Encrypting an Excel File

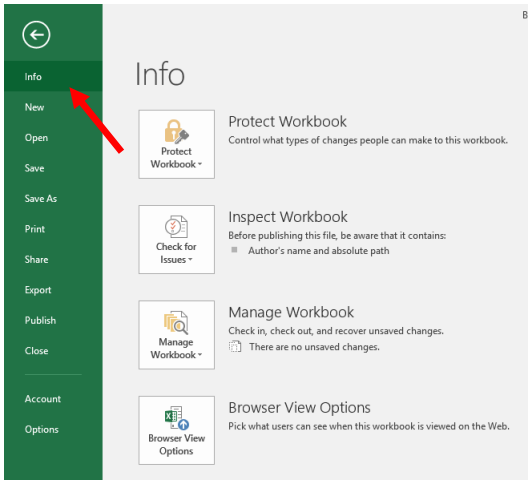
Step 1

- To Encrypt an Excel document that you have created click on File.



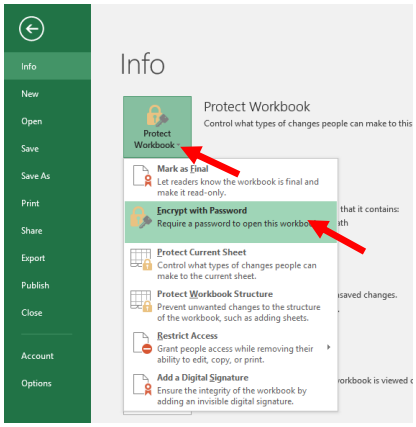
Step 2

- Click on Info.



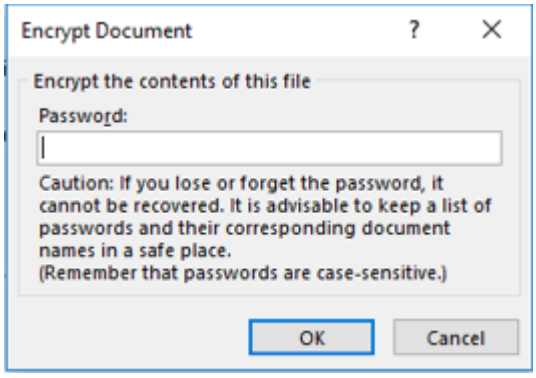
Step 3

- Click on the drop down arrow on Protect Document.
- Click on Encrypt with Password.



Step 4

- Enter the password you wish to use to open this document.



- Click on OK.

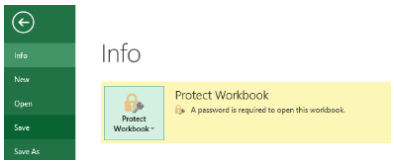
Step 5

- Re-enter password.

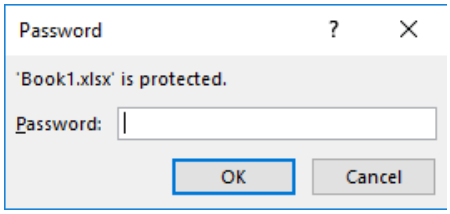
Step 6

- Your document is now protected and will require the password to be entered to open it.

- Click on OK.



- Next time you open your protected document you will be prompted to enter the password.



Appendix 6. Information Records Management Society Retention Guidelines (see separate pdf document)