Data Protection Policy

MANOR HALL ACADEMY TRUST

Approved by:	Directors.	**Date:**	21/05/18.
Last reviewed on:	21/05/18.		
Next review due by:	May 2019.		

Contents

1. Aims 2
2. Legislation and guidance 3
3. Definitions 3
4. Information Classification and Protective Marking 4
5. The data controller 6
6. Roles and responsibilities 7
7. Data protection principles 7
8. Privacy Notice 8
9. Collecting personal data 8
10. Sharing personal data 9
11. Subject access requests and other rights of individuals 9
12. Parental requests to see the educational record 11
13. Biometric recognition systems 11
14. CCTV 11
15. Photographs and videos 11
16. Data protection by design and default 12
17. Data security and storage of records 12
18. Disposal of records 13
19. Personal data breaches 13
20. Training 13
21. Risk Assessments 13
22. Monitoring arrangements 14
23. Use of Cloud Services 14
24. Links with other policies 14
Appendix 1: Personal data breach procedure 16
Appendix 2: Privacy Notice 18

1. Aims

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

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

2. Legislation and guidance

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

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

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

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

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

3. Definitions

Term	Definition
Personal data	Any information relating to an identified, or identifiable, individual. This may include the individual's: • Name (including initials) • Identification number • Location data • Online identifier, such as a username It may also include factors specific to the individual's physical, physiological, genetic, mental, economic, cultural or social identity.
Special categories of personal data	Personal data which is more sensitive and so needs more protection, including information about an individual's: • Racial or ethnic origin • Political opinions • Religious or philosophical beliefs • Trade union membership • Genetics • Biometrics (such as fingerprints, retina and iris patterns), where used for identification purposes • Health – physical or mental • Sex life or sexual orientation
Processing	Anything done to personal data, such as collecting, recording, organising, structuring, storing, adapting, altering, retrieving, using, disseminating, erasing or destroying. Processing can be automated or manual.

Data subject	The identified or identifiable individual whose personal data is held or processed.
Data controller	A person or organisation that determines the purposes and the means of processing of personal data.
Data processor	A person or other body, other than an employee of the data controller, who processes personal data on behalf of the data controller.
Personal data breach	A breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data.

4. Information Classification and Protective Marking

Government has revised the Protective Marking Scheme (April 2014). All the Manor Hall Academy Trust information will be classified into one of the following categories:

NOT PROTECTIVELY MARKED	OFFICIAL	OFFICIAL - SENSITIVE
Information that is published by the Trust, its schools, or made available to the public, or that is freely available.	The majority of information that is created or processed by the Trust and its schools, including that related to routine business operations and services, some of which could have damaging consequences if lost, stolen or published in the media.	A limited subset of OFFICIAL information that could have more damaging consequences (for individuals, the Trust or its schools) if it were lost, stolen or published in the media, where there is clear and justifiable requirement to reinforce the 'need to know'.

The classification NOT PROTECTIVELY MARKED

This applies only to information that rightly belongs in the public domain. This includes:

- Information that the trust/school publishes, for example on its website;
- Other information the trust/school makes available to its community or members of the public, even though it does not routinely publish it;
- Other information the trust/school holds that is freely available

There is no requirement to explicitly mark information with the classification NOT PROTECTIVELY MARKED.

The classification OFFICIAL

All routine business operations and services should be treated as OFFICIAL. The OFFICIAL classification covers information relating to the following:

- The day to day business of the trust/schools, service delivery and public finances;
- Safety, security and resilience;
- Commercial interests, including information provided in confidence and intellectual property;
- Individual people – personal information that must be protected under the Data Protection Act 1998 or other legislation (eg health record).

The word OFFICIAL should be written in capital letters when it is being used as a term to classify information.

The classification OFFICIAL-SENSITIVE

Some information which falls within the scope of the OFFICIAL classification may need a higher degree of protection than would normally be applied. This stronger classification is OFFICIAL-SENSITIVE and applies when:

- There could be more serious consequences (for individuals, the Trust or it schools) in the event that the information is lost, stolen or published in the media;
- There is a clear and justifiable requirement to restrict access solely to those who have a business need to know the information and are within the trusted group.

The OFFICIAL-SENSITIVE classification covers the following:

- Particularly sensitive information relating to identifiable individuals, where inappropriate access could have damaging consequences (for example, information related to health, sex life or sexual orientation, biometrics, genetics, trade union membership, religious or philosophical beliefs, political opinions, racial or ethnic origin, disciplinary proceedings).
- Commercially sensitive information (for example, related to contracts or financial matters).
- Information that if disclosed inappropriately could compromise the operation effectiveness, internal stability or security of the trust and its schools.

The OFFICAL-SENSITIVE classification also applies to all information which is due to be destroyed.

The phrase OFFICAL-SENSITIVE should be written in capital letters when it is being used as a term to classify information and should be clearly and obviously marked.

Information combined from different sources

When information assets are gather together from different sources, it may be the case that the individual items will have different security classifications. In these cases, the overall collection of documents must carry the highest level of classification from the individual items.

Additional guidance

Most pupil or staff personal data that is used within educational institutions will come under the OFFICIAL classification. However, some data eg the home address of a child at risk will be marked OFFICIAL-SENSITIVE.

The Trust will ensure that all school staff, independent contractors working for it, and delivery partners, comply with restrictions applying to the access to, handling and storage of data classified as OFFICIAL or higher.

When information is acquired or created, consideration must be given to how it should be classified.

All information classified as OFFICIAL-SENSITIVE must be clearly and obviously marked with its classification, and any additional descriptors (as described above) should be added if appropriate.

Consideration should be given to whether or not OFFICIAL information needs to be marked with its classification. For example, if it is considered necessary to draw attention to the fact that the information would not be expected to appear in the public domain the OFFICIAL marking should be applied.

All documents (manual or digital) that are to be marked with a classification will be labelled clearly with the wording ‘DOCUMENT CONTROL’ in the footer accompanied by the appropriate classification ie ‘DOCUMENT CONTROL: OFFICIAL_SENSITIVE.

Below are some examples of document control classifications for typical data processed in school.

Typical Information		Document Control
School life and events	School term times, holiday, training days, the curriculum, sports events and results, extra-curricular activities, displays of pupils work, lunchtime menus, extended services, parent consultation, homework and resources, school prospectus.	Most of this information will fall into the NOT PROTECTIVELY MARKED category.
Learning and achievement	Information on how parents can support their individual child’s learning, academic achievement, assessments, attainment, progress with learning, behavior, IEPs.	Most of this information will fall into the OFFICIAL category. There may be learners whose personal data requires an OFFICIAL-SENSITIVE marking eg

		the home address of a child at risk.
Safeguarding	Information pertinent to child protection issues	Most of this information will fall into the OFFICIAL-SENSITIVE category, as it should only ne access on a 'need-to-know' basis.

Information must be stored securely in order to prevent unauthorised access. Stored information should be appropriately backed up to protect it against loss.

Access to information classified as OFFICIAL and OFFICIAL-SENSITVE must be limited to those authorised to view it. Access must be granted only to those who require it in order to perform their jobs. OFFICIAL and OFFICIAL-SENSITIVE information must always be protected against unauthorised access. This means that users must be required to supply a user name and password, or equivalent, in order to gain access to the information.

Documents must also be securely destroyed after use, eg shredded. Destruction markings should also be included in the footer ie 'Securely destroy after use.

Information that is protectively marked up must keep its protective marking when it is printed, copied or transferred to portable media. Protective marked information should be printed, copied or transferred to portable media only when necessary. All protectively marked media in portable form must be protected in transit and stored securely; it must not be left unattended without protection. For advice on encryption please contact a member of the ICT Team.

Below are some examples of different uses of technology and protective marking for typical data processed in school.

Typical Information		The Technology	Notes on Protect markings
School life and events	School term times, holiday, training days, the curriculum, sports events and results, extra-curricular activities, displays of pupils work, lunchtime menus, extended services, parent consultation events.	Common practice is to use publically accessible technology such as school websites or portal, emailed newsletters, subscription text services	Most of this information will fall into the NOT PROTECTIVELY MARKED category.
Learning and achievement	Individual pupil academic, social and behavioural achievements, progress with learning, learning behaviour, how parents can support their child's learning, assessments, attainments, attendance, individual and personalised curriculum and educational needs.	Typically schools will make information available by parents logging on to a system with appropriately secure access, such as a Learning Platform or portal, or by communication to a personal device or email account belonging to the parent.	Most of this information will fall into the OFFICIAL category. There may be pupils whose personal data requires an OFFICIAL-SENSITIVE marking eg the home address of a child at risk. In this case, the school may decide not to make this pupil record available in this way.
Messages and alerts	Attendance, behavioural, achievement, sickness, school closure, transport arrangements and other information that it may be important to inform or contact a parent about as soon as possible. This may be particularly important when it is necessary to contact a parent concerning information that may be considered too sensitive to make available using other online means.	Email and text messaging are commonly used by schools to contact and keep parents informed. Where parents are frequently accessing information online then systems e.g. Learning Platforms or portals, might be used to alert parents to issues via dashboards of information, or be used to provide further detail and context.	Most of this information will fall into the OFFICIAL category. However, since it is not practical to encrypt email or text messages to parents, schools should not send detailed personally identifiable information. General, anonymous alerts ie about school closures would fall into the NOT PROTECTIVELY MARKED category.

5. The data controller

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

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

6. Roles and responsibilities

The Board of trustees have overall responsibility for compliance with the GDPR.

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

6.1 Local Advisory Board (LAB)

The LAB has overall responsibility for ensuring that the academy complies with all relevant data protection obligations.

6.2 Data protection officer

The data protection officer (DPO) is responsible for overseeing the implementation of this policy, monitoring our compliance with data protection law, and developing related policies and guidelines where applicable.

They will provide an annual report of their activities directly to the 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.

Our DPO is Mrs T Lawlor and is contactable via trina.lawlor@manorhall.academy

6.3 Headteacher

The headteacher's act as the representative of the data controller on a day-to-day basis.

6.4 All staff

Staff are responsible for:

- Collecting, storing and processing any personal data in accordance with this policy
- Informing the school of any changes to their personal data, such as a change of address
- Contacting the DPO in the following circumstances:
    - With any questions about the operation of this policy, data protection law, retaining personal data or keeping personal data secure
    - If they have any concerns that this policy is not being followed
    - If they are unsure whether or not, they have a lawful basis to use personal data in a particular way
    - If they need to rely on or capture consent, draft a privacy notice, deal with data protection rights invoked by an individual, or transfer personal data outside the European Economic Area
    - If there has been a data breach
    - Whenever they are engaging in a new activity that may affect the privacy rights of individuals
    - If they need help with any contracts or sharing personal data with third parties

7. Data protection principles

The GDPR is based on data protection principles that our school 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 school aims to comply with these principles.

8. Privacy Notice

8.1 Privacy Notice – Information to Parents/Carers (Appendix 2)

Our schools will inform Parents/Carers of all pupils of the data they collect, process and hold on the pupils, the purposes for which the data is held and the third parties such as the Local Authority and Dfe to whom it may be passed. This privacy notice will be passed to Parents/Carers through a specific letter and will be available on the school's website.

8.2 Privacy Notice – Information to School Workforce (Appendix 2)

The Trust will inform all staff of the data it collects, processes and holds about them, the purposes for which the data is held and the third parties such as the Local Authority and the DfE to whom it may be passed. This Privacy Notice will be passed to staff through a specific letter. New staff joining our Trust will be provided with the Privacy Notice as part of their induction process.

9. Collecting personal data

9.1 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**

For special categories of personal data, we will also meet one of the special category conditions for processing which are set out in the GDPR and Data Protection Act 2018.

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

If we offer online services to pupils, and we intend to rely on consent as a basis for processing, we will get parental consent where the pupil is under 13 (except for online counselling and preventive services).

9.2 Limitation, minimisation and accuracy

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

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

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

When staff no longer need the personal data they hold, they must ensure it is deleted or anonymised. This will be done in accordance with the school's [record retention schedule/records management policy].

Note: if you do not have a record retention schedule or records management policy, you may wish to refer instead to the Information and Records Management Society's toolkit for schools in the final sentence above.

10. 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
- 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.

11. Subject access requests and other rights of individuals

11.1 Subject access requests

Individuals have a right to make a 'subject access request' to gain access to personal information that the school holds about them. This includes:

- Confirmation that their personal data is being processed
- Access to a copy of the data
- The purposes of the data processing
- The categories of personal data concerned
- Who the data has been, or will be, shared with
- How long the data will be stored for, or if this isn't possible, the criteria used to determine this period
- The source of the data, if not the individual
- Whether any automated decision-making is being applied to their data, and what the significance and consequences of this might be for the individual

Subject access requests must be submitted in writing, either by letter, email or fax to the Headteacher. All access requests should be logged with 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.

11.2 Children and subject access requests

Personal data about a child belongs to that child, and not the child's parents or carers. For a parent or carer to make a subject access request with respect to their child, the child must either be unable to understand their rights and the implications of a subject access request, or have given their consent.

Children below the age of 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 our school 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 our school 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.

11.3 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.

11.4 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 Headteacher. All requests should be logged with the DPO. If staff receive such a request, they must immediately forward it to the DPO.

12. Parental requests to see the educational record

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

Although as an academy there is no automatic parental right of access to the educational record, but we may choose to provide this information within 15 school days of receipt of a written request. Charges may apply appropriate to the request.

13. Biometric recognition systems

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

Where we use pupils' biometric data as part of an automated biometric recognition, we will comply with the requirements of the Protection of Freedoms Act 2012.

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

Parents/carers and 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's parent(s)/carer(s).

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

14. 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 headteacher.

15. Photographs and videos

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

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.

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.

See our safeguarding policy/code of conduct policy for more information on our use of photographs and videos.

16. Data protection by design and default

We will put measures in place to show that we have integrated data protection into all of our data processing activities, including:

- Appointing a suitably qualified DPO, and ensuring they have the necessary resources to fulfil their duties and maintain their expert knowledge
- Only processing personal data that is necessary for each specific purpose of processing, and always in line with the data protection principles set out in relevant data protection law (see section 6)
- Completing 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 on this process)
- Integrating data protection into internal documents including this policy, any related policies and privacy notices
- Regularly training members of staff on data protection law, this policy, any related policies and any other data protection matters; we will also keep a record of attendance
- Regularly conducting reviews and audits to test our privacy measures and make sure we are compliant
- Maintaining records of our processing activities, including:
    - For the benefit of data subjects, making available the name and contact details of our school and DPO and all information we are required to share about how we use and process their personal data (via our privacy notices)
    - For all personal data that we hold, maintaining an internal record of the type of data, data subject, how and why we are using the data, any third-party recipients, how and why we are storing the data, retention periods and how we are keeping the data secure

17. Data security and storage of records

We will protect personal data and keep it safe from unauthorised or unlawful access, alteration, processing or disclosure, and against accidental or unlawful loss, destruction or damage.

In particular:

- Paper-based records and portable electronic devices, such as laptops and hard drives that contain personal data are kept under lock and key when not in use

- Papers containing confidential personal data must not be left on office and classroom desks, on staffroom tables, pinned to notice/display boards, or left anywhere else where there is general access
- Where personal information needs to be taken off site, staff must sign it in and out from the school office
- Passwords that are at least 8 characters long containing letters and numbers are used to access school computers, laptops and other electronic devices. Staff and pupils 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 governors who store personal information on their personal devices are expected to follow the same security procedures as for school-owned equipment (see our [online safety policy/ICT policy/acceptable use agreement/policy on acceptable use])
- 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)

18. Disposal of records

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

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

19. Personal data breaches

The 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

20. Training

All staff and governors are provided with data protection training as part of their induction process.

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

21. Risk Assessments

Information Risk Assessments will be carried out by Information Asset Owners to establish the security measures already in place and whether they are the most appropriate. The risk assessments will involve:

- Recognising the risks that are present
- Judging the level of the risks (both the likelihood and consequences; and
- Prioritising the risks

Risk assessments are an ongoing process.

22. 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 **every 2 years** and shared with the full governing board.

Note: the 2-year review frequency here reflects the information in the Department for Education's advice on statutory policies. While the GDPR and Data Protection Act 2018 (when in place) are still new and schools are working out how best to implement them, you may wish to review your data protection policy annually, and then extend this to every 2 years once you are confident with your arrangements.

23. Use of Cloud Services

When using any cloud based services, the Trust will ensure that our schools meet all of their obligations under the DPA, ensuring full compliance with the eight Data Protection Principles. Whilst school and pupil data may be stored and controlled in the cloud by a supplier, responsibility for all areas of data protection compliance still rests with the school.

The Trust schools use the Microsoft Office 365 cloud service. This service provides email, calendars, file storage and more for both pupils and staff. PSFinancial Cloud for the finance system.

Below is a list of questions that the Trust considered when selecting our preferred cloud services provider.

- Where is the data stored?
- How often is the data backed up?
- Does the service provider have a clear process for recovering data?
- How does the service provider protect your privacy?
- Who owns the data that you store on the platform?
- Who has access to the data?
- Is personal information shared with anyone else?
- Does the service provider share contact details with third party advertisers? Or serve users with ads?
- What steps does the service provider take to ensure that your information is secure?
- How reliable is the system?
- What level of support is offered as part of the service?

As of October 2014 the DfE and Information Commissioners Office (ICO) created a self-certification framework for cloud service providers. School are able to use the checklists to support their assessment of the extent to which the cloud services from a particular supplier meet their educational, technical and commercial needs in a DPA-compliant manner. The Microsoft response to the self-certification framework demonstrates that the Office 365 cloud service allows our schools to meet their obligations under the Data Protection Act.

24. Links with other policies

This data protection policy is linked to our:

- Freedom of information publication scheme
- Safeguarding policy
- Staff Code of Conduct
- E-safety Policy

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 Headteacher who will inform the DPO
- The Headteacher/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 headteacher and the chair of governors
- The headteacher with discussion with the DPO will make all reasonable efforts to contain and minimise the impact of the breach, assisted by relevant staff members or data processors where necessary. (Actions relevant to specific data types are set out at the end of this procedure)
- The DPO will assess the potential consequences, based on how serious they are, and how likely they are to happen
- The DPO will work out whether the breach must be reported to the ICO. This must be judged on a case-by-case basis. To decide, the DPO will consider whether the breach is likely to negatively affect people's rights and freedoms, and cause them any physical, material or non-material damage (e.g. emotional distress), including through:
    - Loss of control over their data
    - Discrimination
    - Identify theft or fraud
    - Financial loss
    - Unauthorised reversal of pseudonymisation (for example, key-coding)
    - Damage to reputation
    - Loss of confidentiality
    - Any other significant economic or social disadvantage to the individual(s) concerned

  If it's likely that there will be a risk to people's rights and freedoms, the DPO must notify the ICO.
- The DPO will document the decision (either way), in case it is challenged at a later date by the ICO or an individual affected by the breach. Documented decisions are stored on the school's computer system.
- Where the ICO must be notified, the DPO will do this via the 'report a breach' page of the ICO website within 72 hours. As required, the DPO will set out:
    - A description of the nature of the personal data breach including, where possible:
        - The categories and approximate number of individuals concerned
        - The categories and approximate number of personal data records concerned
    - The name and contact details of the DPO
    - A description of the likely consequences of the personal data breach
    - A description of the measures that have been, or will be taken, to deal with the breach and mitigate any possible adverse effects on the individual(s) concerned

- If all the above details are not yet known, the DPO will report as much as they can within 72 hours. The report will explain that there is a delay, the reasons why, and when the DPO expects to have further information. The DPO will submit the remaining information as soon as possible
- The DPO will also assess the risk to individuals, again based on the severity and likelihood of potential or actual impact. If the risk is high, the DPO will promptly inform, in writing, all individuals whose personal data has been breached. This notification will set out:
    - The name and contact details of the DPO
    - A description of the likely consequences of the personal data breach
    - A description of the measures that have been, or will be, taken to deal with the data breach and mitigate any possible adverse effects on the individual(s) concerned
- The DPO will notify any relevant third parties who can help mitigate the loss to individuals – for example, the police, insurers, banks or credit card companies
- The DPO will document each breach, irrespective of whether it is reported to the ICO. For each breach, this record will include the:
    - Facts and cause
    - Effects
    - Action taken to contain it and ensure it does not happen again (such as establishing more robust processes or providing further training for individuals)

  Records of all breaches will be stored on the school's computer system. The DPO and headteacher will meet to review what happened and how it can be stopped from happening again. This meeting will happen as soon as reasonably possible

Actions to minimise the impact of data breaches

We will take the actions set out below to mitigate the impact of different types of data breach, focusing especially on breaches involving particularly risky or sensitive information. We will review the effectiveness of these actions and amend them as necessary after any data breach.

Sensitive information being disclosed via email (including safeguarding records)

- *If special category data (sensitive information) is accidentally made available via email to unauthorised individuals, the sender must attempt to recall the email as soon as they become aware of the error*
- *Members of staff who receive personal data sent in error must alert the sender and the DPO as soon as they become aware of the error*
- *If the sender is unavailable or cannot recall the email for any reason, the DPO will ask the ICT department to recall it*
- *In any cases where the recall is unsuccessful, the DPO will contact the relevant unauthorised individuals who received the email, explain that the information was sent in error, and request that those individuals delete the information and do not share, publish, save or replicate it in any way*
- *The DPO will ensure we receive a written response from all the individuals who received the data, confirming that they have complied with this request*
- *The DPO will carry out an internet search to check that the information has not been made public; if it has, we will contact the publisher/website owner or administrator to request that the information is removed from their website and deleted*

Other types of breach could include:

- *Details of pupil premium interventions for named children being published on the school website*
- *Non-anonymised pupil exam results or staff pay information being shared with governors*
- *A school laptop containing non-encrypted sensitive personal data being stolen or hacked*
- *The school's cashless payment provider being hacked and parents' financial details stolen*

Privacy Notice

Privacy Notices are available to view or download on each academies website.