Data Protection (GDPR) Policy

Reviewed by the Estates, Health & Safety Committee:	Summer 2025
Adopted by the Governing Body:	Spring 2026
To be Reviewed:	Spring 2027

All stakeholders are responsible for reporting known breaches internally to a senior manager or to the Data Protection Officer as soon as the breach is recognised. The responsible member of the senior leadership team should be informed.

24.3. The Academy will keep and implement a dedicated Data Breach Procedure to ensure any personal data breaches, including the facts relating to the data breach, its effects and the remedial action taken, are recorded in a data breach log and acted on accordingly. Individuals will also be informed of their right to escalate complaints to the ICO if they feel organisational handling was inadequate, in line with the Data Use and Access Act 2025.

24.4. The log shall be monitored and assessed by the Data Protection Officer. It will enable them to verify compliance with the data breach rules and raise awareness of minor breaches that may assist in identifying new data handling processes and training requirements.

24.5. In the case of a personal data breach resulting in a likely risk to the rights and freedoms of natural personals, and after consultation with the Data Protection Officer, the Academy shall, without undue delay and, where feasible, not later than 72 hours after having become aware of it, notify the personal data breach to the Information Commissioner's Office.

CONTENTS PAGE

All stakeholders are responsible for reporting known breaches internally to a senior manager or to the Data Protection Officer as soon as the breach is recognised. The responsible member of the senior leadership team should be informed.

'We promise to shine together'

Let the light of your face shine upon us - Psalm 4:6

Our ambition is to serve our community by providing an excellent education, which is inclusive and distinctive within the context of Christian belief and practice, upholding our values in the daily life of the Academy and in our relationships with others.

All stakeholders are responsible for reporting known breaches internally to a senior manager or to the Data Protection Officer as soon as the breach is recognised. The responsible member of the senior leadership team should be informed.

COMMITMENT TO GENERAL DATA PROTECTION AND DATA PROTECTION BY DESIGN

1. Data Protection Act 2018 (DPA) is the law that protects personal privacy and upholds individual rights in relation to data protection. It applies to anyone who handles or has access to people's personal data. This policy also complies with the Data Use and Access Act 2025, which strengthens transparency requirements and introduces enhanced rights for individuals, including the right to accessible complaint pathways.

1.1. This policy is intended to ensure that personal information is dealt with properly and securely and in accordance with the legislation. It will apply to personal information regardless of the way it is used, recorded and stored and whether it is held in paper files or electronically.

1.2. This policy sets out the Academy's commitment to GDPR and the implementation of a data protection by design approach.

1.3. The Academy will refer to documents and guidance from the Information Commissioner's Office and the Department for Education in relation to GDPR and data processing.

1.4. This includes ensuring the following:

- Assigning a link Governor;
- Assigning responsibility to an individual within the Academy;
- Assigning a DPO;
- Ensuring that all staff are trained annually, in data protection and take responsibility for the collection, processing, storage and destruction of data;
- A lawful basis for processing is documented for all processing activity;

All stakeholders are responsible for reporting known breaches internally to a senior manager or to the Data Protection Officer as soon as the breach is recognised. The responsible member of the senior leadership team should be informed.

- Principles relating to processing of personal data are adhered to;
- The rights of data subjects are respected;
- Risks to the rights of data subjects are assessed and mitigated for all large-scale and new processing;
- Regular independent reviews of processing activity and processing documentation are carried out;
- Organisational and technical measures are implemented to protect data;
- Data breaches impacting on the rights and freedoms of data subjects will be reported to the Information Commissioner's Office (ICO).

2. POLICY OBJECTIVES ROLES RESPONSIBILITIES

2.1. The Academy as the Data Controller will comply with its obligations under the GDPR and the Data Protection Act 2018. The Academy is committed to being concise, clear and transparent about how it obtains and uses personal information and will ensure data subjects are aware of their rights under the legislation. This policy sets out how the Academy will do this.

2.2. All Academy staff and the Academy workforce must have a general understanding of the law and understand how it may affect their decisions in order to make an informed judgement about how information is gathered, used and ultimately deleted. All staff must read, understand and comply with this policy in order to comply with its obligations under GDPR and the Data Protections Act 2018.

2.3. The Information Commissioner as the Regulator can impose substantial fines for breaches of GDPR and the Data Protection Act 2018 and other Data Protection Legislation. Therefore it is imperative that the Academy, all staff and the workforce comply with the legislation. The DPO will be the principal point of contact with the ICO.

All stakeholders are responsible for reporting known breaches internally to a senior manager or to the Data Protection Officer as soon as the breach is recognised. The responsible member of the senior leadership team should be informed.

3. POLICY STATEMENT

3.1. Everyone has rights with regard to the way in which their personal data is handled. During the course of our activities as an Academy we will collect, store and process personal data about our pupils, workforce, parents/carers and others. This makes us a data controller in relation to that personal data.

3.2. We are committed to the protection of all personal data and special category personal data for which we are the data controller.

3.3. The law imposes significant fines for failing to lawfully process and safeguard personal data and failure to comply with this policy may result in those fines being applied.

3.4. All members of our staff and workforce will comply with this policy when processing personal data on our behalf. Any breach of this policy may result in disciplinary or other action.

4. ABOUT THIS POLICY

4.1. The types of personal data that we may be required to handle include information about pupils, parents/carers, our workforce, and others that we deal with. The personal data which we hold is subject to certain legal safeguards specified in the General Data Protection Regulation the Data Protection Act 2018, and other regulations Data Protection Legislation.

4.2. This policy does not form part of any employee's contract of employment and may be amended at any time.

4.3. This policy sets out rules on data protection and the legal conditions that must be satisfied when the Academy processes personal data.

All stakeholders are responsible for reporting known breaches internally to a senior manager or to the Data Protection Officer as soon as the breach is recognised. The responsible member of the senior leadership team should be informed.

4.4. This policy, combined with the Academy's privacy notices and any other document referred to herein, sets out the basis on which the Academy will process any personal data collected from data subjects, or provided to us by data subjects directly and or from other sources.

5. DATA PROTECTION OFFICER

5.1. As an Academy we are required to appoint a Data Protection Officer James England ("DPO") . Our DPO is Data Protection Education and they can be contacted at dpo@dataprotection.education. The DPO is responsible for ensuring compliance with the Data Protection Legislation and with this policy. Any questions about the operation of this policy or any concerns that the policy has not been followed should be referred in the first instance to the DPO.

5.2. The Academy shall maintain a DPO to represent the rights of data subjects and a named Data Protection lead in order to assist the DPO.

5.3. The Academy shall ensure that the DPO is involved properly and in a timely manner, in all issues which relate to the protection of personal data.

5.4. The Academy shall support the DPO in performing the responsibilities outlined below by providing resources necessary to carry out those tasks and access to personal data and processing operations. The DPO shall maintain his or her expert knowledge.

5.5. The Academy shall ensure that the DPO does not receive any instructions regarding the exercise of their tasks. They shall not be dismissed or penalised by the controller or the processor for performing his tasks.

5.6. The DPO shall directly report to the highest management level of the Academy, as needed and report to the Governing Body at least once a year.

5.7. Data subjects may contact the DPO with regard to all issues related to processing of their personal data and to the exercise of their rights under the regulations.

All stakeholders are responsible for reporting known breaches internally to a senior manager or to the Data Protection Officer as soon as the breach is recognised. The responsible member of the senior leadership team should be informed.

5.8. The DPO and the Data Protection Lead will be bound by confidentiality and must maintain data security by protecting the confidentiality, integrity and availability of all personal data, defined as follows:

- **Confidentiality** means that only people who have a need to know and are authorised to use the personal data can access it.
- **Integrity** means that personal data is accurate and suitable for the purpose for which it is processed.
- **Availability** means that only authorised users can access the personal data when they need it for authorised purposes.

5.9. The DPO shall have the following responsibilities:

- Review of all data processing activities (inventory/mapping);
- Conduct of regular health checks/audits and issue recommendations;
- Assist with data protection impact assessments and monitoring performance;
- Monitoring and advice relating to subject access requests and data breaches;
- Assist the Academy with maintenance of records;
- Monitoring and advice relating to FOi and other information requests;
- Cooperation with, and acting as the contact point for the Information Commissioner's Office, who are the supervisory authority in respect of all data protection matters;
- Act as the contact point for data subjects to deal with requests and complaints;
- Training of Academy staff and workforce.

6. DATA PROTECTION PRINCIPLES

6.1. Anyone processing personal data must comply with the data protection principles. The Academy will comply and is committed to these principles in relation to any processing of personal data. The Data

All stakeholders are responsible for reporting known breaches internally to a senior manager or to the Data Protection Officer as soon as the breach is recognised. The responsible member of the senior leadership team should be informed.

Protection principles provide that personal data must be:

- **Processed lawfully, fairly and in a transparent manner** in relation to the data subject and their rights;
- **Collected for specified, explicit and legitimate purposes** and not further processed in a manner that is incompatible with those purposes;
- **Adequate, relevant and limited to what is necessary** in relation to the purposes for which they are processed;
- **Accurate and, where necessary, kept up to date;**
- **Kept in a form which permits identification of data subjects for no longer than is necessary;**
- **Processed in a manner that ensures appropriate security of the personal data;**
- **Must NOT be transferred to people or organisations situated in other countries without adequate protection.**

7. DATA SUBJECT'S RIGHTS

7.1. The Academy supports the rights of data subjects {or the parents/carers of data subjects where data subjects are not able to demonstrate the capacity to understand their rights) in relation to data that is processed or stored about them, as follows:

- Right to fair and transparent processing;
- Right of access;
- Right of rectification;
- Right to erasure {the "right to be forgotten");
- The right to restrict processing;
- Right to be notified of erasure, rectification or restriction;
- Right of data portability;
- Right to object to processing;
- Right to object to processing for the purposes of direct marketing;

All stakeholders are responsible for reporting known breaches internally to a senior manager or to the Data Protection Officer as soon as the breach is recognised. The responsible member of the senior leadership team should be informed.

- Right to object to processing for scientific, historical or statistical purposes;
- Right to not be evaluated on the basis of automated processing;
- Right to withdraw consent at any time;
- Right to be notified about a data breach;
- Right to an effective judicial remedy against a supervisory authority;
- Right to lodge a complaint with supervisory authority;
- Right to an effective judicial remedy against a controller or processor;
- Right to compensation.

The Academy shall maintain procedures, policies and notices to ensure that data subjects are informed about their rights.

8. FAIR AND TRANSPARENT PROCESSING OF DATA

8.1. Data Protection Legislation is not intended to prevent the processing of personal data, but to ensure that it is done fairly and without adversely affecting the rights of the data subject.

8.2. For personal data to be processed fairly, data subjects must and will be made aware of the following in our privacy notices or requests to process data:

- That the personal data is being processed;
- Why the personal data is being processed;
- What the lawful basis is for that processing (see below);
- Whether the personal data will be shared, and if so with whom;
- The period for which the personal data will be held;
- The existence of the data subject's rights in relation to the processing of that personal data; and
- The right of the data subject to raise a complaint with the Information Commissioner's Office in relation to any processing.

All stakeholders are responsible for reporting known breaches internally to a senior manager or to the Data Protection Officer as soon as the breach is recognised. The responsible member of the senior leadership team should be informed.

8.3. The Academy will only process data that is **necessary and relevant to the purpose for which it was gathered, and will ensure that we have a lawful basis for any processing.**

8.4. Data collected for the purposes of public health will be kept as long as required. Contact data for visitors will be kept for 21 days after the most recent visit, with information on visitors kept as per standard retention requirements. Public Health data may be shared with third-parties as required including, but not limited to:

- National Health Service
- Public Health England
- Other local health authorities

8.5. Data collected and processed for public health purposes is done so under GDPR Article 9(2)(i) which states: (in part) "processing is necessary for reasons of public interest in the area of public health, such as protecting against serious cross-border threats to health..." and Recital 54 which includes: "The processing of special categories of personal data may be necessary for reasons of public interest in the areas of public health without consent of the data subject."

8.6. Collection and processing of visitor data will be documented in the privacy notices and in a statement available to visitors at the time of data collection to include the following information:

8.7. "We collect the following visitor information for the purposes of security, safety and public health:

- Name
- Academy
- Date and time of visit
- Contact details

All stakeholders are responsible for reporting known breaches internally to a senior manager or to the Data Protection Officer as soon as the breach is recognised. The responsible member of the senior leadership team should be informed.

8.8. These are kept for six years in case of any claims by pupils, staff or visitors under the Limitations Act (1980}.

8.9. Contact details will be deleted after 21 days.

8.10. For further details, please see our Data Protection Policy, or contact our Data Protection Officer"

9. LAWFUL PROCESSING OF DATA

9.1. For personal data to be processed lawfully it must be processed on the basis on one of the legal grounds set out in the DATA Protection Legislation. The Academy will only process personal data where a lawful basis for processing exists. Specifically, where:

- The data subject has given **consent** to the processing of his or her personal data for one or more specific purposes;
- Processing is necessary for the **performance of a contract** to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract;
- Processing is necessary for compliance with a **legal obligation** to which the controller is subject (e.g the Education Act 2011};
- Processing is necessary in order to protect the **vital interests** of the data subject or of another natural person;
- Processing is necessary for the **performance of a task carried out in the public interest** or in the exercise of official authority vested in the controller.

10. SPECIAL CATEGORY DATA

10.1. This is data relating to **health; race; sexuality; religion; criminal offences; political opinions and union memberships.**

All stakeholders are responsible for reporting known breaches internally to a senior manager or to the Data Protection Officer as soon as the breach is recognised. The responsible member of the senior leadership team should be informed.

10.2. These special categories of personal data relating to will not be processed unless a specific lawful basis as listed in Article 9 of the GDPR applies. When this special category data is being processed we will normally only do so under the following legal grounds:

- Where the processing is **necessary for employment law** purposes, for example in relation to sickness absence;
- Where the processing is necessary for reasons of substantial public interest, for example for the purposes of equality of opportunity and treatment;
- Where the processing is necessary for **health or social care purposes,** for example in relation to pupils with medical conditions or disabilities; and
- **Where none of the above apply then we will seek the consent of the data subject to the processing of their special category personal data.**

11. CONSENT

11.1. There are strict legal requirements in relation to the form of consent that must be obtained from data subjects.

11.2. When pupils, staff or our workforce join the Academy a consent form will be required to be completed in relation to them. This consent form deals with:

- Legal name;
- Contact details;
- Emergency contact details;
- Medical/Dietary information.

11.3. Where appropriate third parties may also be required to complete a consent form.

All stakeholders are responsible for reporting known breaches internally to a senior manager or to the Data Protection Officer as soon as the breach is recognised. The responsible member of the senior leadership team should be informed.

11.4. In relation to all pupils under the age of 12 years old we will seek consent from an individual with parental responsibility for that pupil.

11.5. We will generally only seek consent directly from a pupil if they are legally able to give such consent. The legal age for consent under Data Protection legislation is 12. However we recognise that this may not be appropriate in certain circumstances and therefore the Academy may be required to seek consent from an individual with parental responsibility.

11.6. If consent is required for the processing of personal data of any data subject then the form of this consent must:

- Inform the data subject of exactly what we intend to do with their personal data;
- Require them to positively confirm that they consent (we cannot ask them to opt-out rather than opt-in); and
- Inform the data subject of how they can withdraw their consent.

11.7. Any **consent must be freely given,** which means that we cannot make the provision of any goods or services or other matter conditional on a data subject giving their consent.

11.8. The DPO must always be consulted in relation to any consent form before consent is obtained.

11.9. A record must always be kept of any consent, including how it was obtained and when.

11.10. There may be circumstances where it is considered necessary to process personal data or special category personal data in order to protect the vital interests of a data subject. This might include safeguarding, child protection and medical emergencies where the data subject is not in a position to give consent to the processing. We believe that this will only occur in very specific and limited circumstances. In such circumstances we would usually seek to consult with the DPO in advance,

All stakeholders are responsible for reporting known breaches internally to a senior manager or to the Data Protection Officer as soon as the breach is recognised. The responsible member of the senior leadership team should be informed.

12. DISCLOSURE AND SHARING OF PERSONAL INFORMATION

12.1. We may share personal data that we hold about data subjects, with other organisations, without consent, where we have a lawful basis for doing so. Such organisations include the Department for Education and Education and Skills Funding Agency "ESFA", Ofsted, health authorities and professionals, the Local Authority, examination bodies, other organisations, and other organisations where we have a lawful basis for doing so.

12.2. The Academy will inform data subjects of any sharing of their personal data unless we are not legally required to do so, for example where personal data is shared with the police in the investigation of a criminal offence.

12.3. In some circumstances we will not share safeguarding information. Please refer to our Safeguarding and Child Protection Policy.

12.4. Further detail is provided in our Record of Processing Activities.

13. DATA SECURITY

13.1. The Academy will implement appropriate data security measures using policies, procedures and technologies to ensure and maintain the security of all personal data from the point of collection to the point of destruction.

All stakeholders are responsible for reporting known breaches internally to a senior manager or to the Data Protection Officer as soon as the breach is recognised. The responsible member of the senior leadership team should be informed.

13.2. These security measures will be appropriate to the risks in processing personal data and will be consistent with the rights of the data subjects.

13.3. These measures shall include as appropriate:

- Data access controls to ensure that the Personal Data can only be accessed by authorised personnel for the purposes agreed in the record of processing activity and outlined in the Academy privacy notice;
- In assessing the appropriate level of security, account shall be taken in particular, of all the risks that are presented by processing, for example from accidental or unlawful destruction, loss, or alteration, unauthorised or unlawful storage, processing, access or disclosure of personal data;
- The anonymisation, pseudonymisation and encryption of personal data;
- The ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services;
- The ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident;
- A process for regular testing, assessing, and evaluating the effectiveness of technical and Academic measures for ensuring the security of the processing of personal data;
- Measures to identify vulnerabilities with respect to the processing of personal data in systems used to provide services to the Academy.

14. DATA PROTECTION IMPACT ASSESSMENTS

14.1. The Academy takes data protection very seriously, and will consider and comply with the requirements of Data Protection Legislation in relation to all of its activities whenever these involve the use of personal data, in accordance with the principles of data protection by design and default.

All stakeholders are responsible for reporting known breaches internally to a senior manager or to the Data Protection Officer as soon as the breach is recognised. The responsible member of the senior leadership team should be informed.

14.2. In certain circumstances the law requires us to carry out detailed assessments of proposed processing. This includes where we intend to use new technologies which might pose a high risk to the rights of data subjects because of the types of data we will be processing or the way that we intend to do so.

14.3. The Academy will complete an assessment of any such proposed processing and will use a template document which ensures that all relevant matters are considered.

14.4. The DPO should always be consulted as to whether a data protection impact assessment is required, and if so how to undertake that assessment.

15. DATA BREACHES

15.1. **The Academy will keep and implement a dedicated Data Breach Procedure to ensure any personal data breaches, including the facts relating to the data breach, its effects and the remedial action taken, are recorded in a data breach log and acted on accordingly. Individuals will also be informed of their right to escalate complaints to the ICO if they feel organisational handling was inadequate, in line with the Data Use and Access Act 2025.**

15.2. **The log shall be monitored and assessed by the Data Protection Officer. It will enable them to verify compliance with the data breach rules and raise awareness of minor breaches that may assist in identifying new data handling processes and training requirements.**

15.3. **In the case of a personal data breach resulting in a likely risk to the rights and freedoms of natural personals, and after consultation with the Data Protection Officer, the Academy shall, without undue delay and, where feasible, not later than 72 hours after having become aware of it, notify the personal data breach to the Information Commissioner's Office.**

16. PUBLICATION OF INFORMATION

16.1. The Academy maintains and publishes a publication scheme on its website outlining classes of information that will be made routinely available, including policies and procedures.

16.2. Classes of information specified in the publication scheme will be made available quickly and easily on request.

16.3. The Academy will not publish any personal information, including photos, on its website without the permission of the affected individual.

All stakeholders are responsible for reporting known breaches internally to a senior manager or to the Data Protection Officer as soon as the breach is recognised. The responsible member of the senior leadership team should be informed.

16.4. When uploading information to the Academy website, staff will be considerate of any metadata or deletions which could be accessed in documents and images on the site.

17. DBS DATA

17.1. All data provided by the DBS will be handled in line with data protection legislation; this includes electronic communication.

17.2. Data provided by the DBS will never be duplicated.

17.3. Any third parties who access DBS information will be made aware of the data protection legislation, as well as their responsibilities as a data handler.

17.4. Data Subjects have the right to appeal against any automated decision making, such as a DBS check.

18. PHOTOGRAPHY IMAGES AND VIDEOS

18.1. Photographs and videos will only be collected and stored by the Academy staff and workforce with a documented lawful basis.

18.2. Photographs and videos will normally only be taken and used where they are deemed essential for performing the public task of the Academy or relative to providing education.

18.3. However there may be occasions that arise where the Academy would like to celebrate the achievements of our pupils and therefore we may want to use images and videos of our pupils within promotional materials, or for publication in the media such as local, or even national, newspapers covering Academy events or achievements. If this is the case we will seek the consent of the pupils, and their parents/carers where appropriate, before allowing the use of images or videos of pupils for such purposes.

All stakeholders are responsible for reporting known breaches internally to a senior manager or to the Data Protection Officer as soon as the breach is recognised. The responsible member of the senior leadership team should be informed.

18.4. Where photographs are required for other purposes, these purposes will be documented and explicit consent will be sought.

18.5. The retention period for photographs and videos taken by the Academy staff and workforce will be documented in the Academy retention schedule. At the end of the retention period photographs will either be destroyed or they may be retained as photos for archiving purposes in the public interest.

18.6. Parents/Carers and others attending Academy events are allowed to take photographs and videos of those events for domestic purposes. For example, parents/carers can take video recordings of an Academy performance involving their child. The Academy does not prohibit this as a matter of policy.

18.7. The Academy does not however agree to any such photographs or videos being used for any other purpose, but acknowledges that such matters are, for the most part, outside of the ability of the Academy to control or prevent.

18.8. The Academy asks that parents/carers and others do not post any images or videos which include any child other than their own child on any social media or otherwise publish those images or videos.

18.9. Whenever a pupil begins their attendance at the Academy they, or their parents/carers where appropriate, will be asked to complete a consent form in relation to the use of images and videos of that pupil. We will not use images or videos of pupils for any purpose where we do not have consent.

19. CCTV

19.1. CCTV may be used for the purpose of protecting the safety of staff, pupils and visitors and to help secure the physical premises. Please refer to the Academy's Health & Safety policy.

19.2. Notices of recording including details of the Data Controller and where a copy of the Academy's

All stakeholders are responsible for reporting known breaches internally to a senior manager or to the Data Protection Officer as soon as the breach is recognised. The responsible member of the senior leadership team should be informed.

Health & Safety policy can be obtained will be included on clearly visible signs posted at all entrances to the Academy site.

19.3. All CCTV footage is securely stored and can only be accessed by appropriate members of staff. All images recorded by CCTV will be deleted as defined in the retention schedule.

19.4. Where the Academy installs new additional CCTV cameras, a data privacy impact assessment will be carried out prior to installation.

19.5. The nominated person responsible for CCTV in the Academy is the Operations Manager & ICT Manager with Service Providers Property 360

19.6. Day-to-day management responsibility for deciding what information is recorded, how it is used and who can access it is delegated to the Operations Manager & ICT Manager.

20. RETENTION SCHEDULE

20.1. The Academy will not keep personal data longer than necessary and will maintain a retention schedule outlining the retention requirements of electronic and paper records. The Academy will retain the minimum amount of information that it requires to carry out its statutory functions and the provision of services.

20.2. In circumstances where a retention period of a specific document has expired, checks will be made to confirm disposal and consideration given to the method of disposal to be used based on the data to be disposed of.

20.3. These checks will include the following questions being addressed:

- Have the documents been checked to ensure they are appropriate for destruction?

All stakeholders are responsible for reporting known breaches internally to a senior manager or to the Data Protection Officer as soon as the breach is recognised. The responsible member of the senior leadership team should be informed.

- Is retention required to fulfil statutory obligations or other regulatory obligations, including child protection?
- Is retention required for evidence?
- Is retention required to meet the operational needs of the service?
- Is retention required because the document or record is of historic interest, intrinsic value or required for Academic Memory

21. TRAINING

21.1. The Academy shall ensure that all members of staff receive data protection training, including training on information handling appropriate to ensure data protection competence in their role. This training shall be completed every two years as a minimum.

22. DATA PROCESSORS

22.1. The Academy contracts with various organisations who provide services to the Academy, including:

- Payroll Providers - to enable us to pay our employees;
- Parent payment systems - which enable parents/carers to pay for Academy meals, trips and/or uniforms;
- Financial systems - electronic accounting systems which enable processing of payments;

All stakeholders are responsible for reporting known breaches internally to a senior manager or to the Data Protection Officer as soon as the breach is recognised. The responsible member of the senior leadership team should be informed.

- Pupil Assessment systems - Management Information Systems which support us with the tracking and monitoring of pupils' attendance, contact details, medical data and achievements;
- Communication systems - to enable us to effectively communicate with parent and pupils;
- Photographers - to enable us to store pupil photographs for safeguarding purposes;

22.2. In order that these services can be provided effectively we are required to transfer personal data of data subjects to these data processors.

22.3. Personal data will only be transferred to a data processor if they agree to comply with our procedures and policies in relation to data security, or if they put in place adequate measures themselves to the satisfaction of the Academy.

22.4. The Academy will always undertake due diligence of any data processor before transferring the personal data of data subjects to them.

22.5. Contracts with data processors will comply with Data Protection Legislation and contain explicit obligations on the data processor to ensure compliance with the Data Protection Legislation, and compliance with the rights of Data Subjects.

23. COMPLAINTS AND THE RIGHT TO CHALLENGE DATA USE

23.1. Individuals may complain if they believe their data has been mishandled or their rights infringed.

23.2. Complaints can be submitted in writing, by email, or by phone.

23.3. Complaints will be handled in accordance with our Data Protection Complaints Policy and acknowledged within 5 working days.

All stakeholders are responsible for reporting known breaches internally to a senior manager or to the Data Protection Officer as soon as the breach is recognised. The responsible member of the senior leadership team should be informed.

23.4. A substantive response will be provided within 1 calendar Month.

23.5. If dissatisfied, individuals may escalate to the Information Commissioner's Office and if you remain dissatisfied to the Data Rights Tribunal.

24. MONITORING AND REVIEW ARRANGEMENTS

24.1. The Principal/School Business Manager will be responsible for monitoring the implementation and effectiveness of this policy. It will be reviewed every two years by the Finance, Personnel, Audit and Risk Committee; or before at any time, if there is new relevant legislation or guidance.

All stakeholders are responsible for reporting known breaches internally to a senior manager or to the Data Protection Officer as soon as the breach is recognised. The responsible member of the senior leadership team should be informed.

APPENDIX 1- GDPR DEFINITIONS

Personal data means any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is a person who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or by one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person;

Processing means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, Academy, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction;

Restriction of processing means the marking of stored personal data with the aim of limiting their processing in the future;

Profiling means any form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to a natural person, in particular to analyse or predict aspects concerning that natural person's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements;

Pseudonymisation means the processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is kept separately and is subject to technical and Academyal measures to ensure that the personal data are not attributed to an identified or identifiable natural person;

Filing system means any structured set of personal data which are accessible according to specific criteria, whether centralised, decentralised or dispersed on a functional or geographical basis;

All stakeholders are responsible for reporting known breaches internally to a senior manager or to the Data Protection Officer as soon as the breach is recognised. The responsible member of the senior leadership team should be informed.

Controller means the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data; where the purposes and means of such processing are determined by Union or Member State law, the controller or the specific criteria for its nomination may be provided for by Union or Member State law;

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

Recipient means a natural or legal person, public authority, agency or another body, to which the personal data are disclosed, whether a third party or not. However, public authorities which may receive personal data in the framework of a particular inquiry in accordance with Union or Member State law shall not be regarded as recipients; the processing of those data by those public authorities shall be in compliance with the applicable data protection rules according to the purposes of the processing;

Third party means a natural or legal person, public authority, agency or body other than the data subject, controller, processor and persons who, under the direct authority of the controller or processor, are authorised to process personal data;

Consent of the data subject means any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her;

Personal data breach means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed;

Genetic data means personal data relating to the inherited or acquired genetic characteristics of a natural person which give unique information about the physiology or the health of that natural person and which result, in particular, from an analysis of a biological sample from the natural person in question;

All stakeholders are responsible for reporting known breaches internally to a senior manager or to the Data Protection Officer as soon as the breach is recognised. The responsible member of the senior leadership team should be informed.

Biometric data means personal data resulting from specific technical processing relating to the physical, physiological or behavioural characteristics of a natural person, which allow or confirm the unique identification of that natural person, such as facial recognition software;

Data concerning health means personal data related to the physical or mental health of a natural person, including the provision of health care services, which reveal information about his or her health status;

Enterprise means a natural or legal person engaged in an economic activity, irrespective of its legal form, including partnerships or associations regularly engaged in an economic activity;

Supervisory authority means an independent public authority which is established by a Member State pursuant to Article 51 of the GDPR;

Cross-border processing means either:

- processing of personal data which takes place in the context of the activities of establishments in more than one Member State of a controller or processor in the Union where the controller or processor is established in more than one Member State; or
- processing of personal data which takes place in the context of the activities of a single establishment of a controller or processor in the Union but which substantially affects or is likely to substantially affect data subjects in more than one Member State;
- **Relevant and reasoned objection** means an objection to a draft decision as to whether there is an infringement of this Regulation, or whether envisaged action in relation to the controller or processor complies with this Regulation, which clearly demonstrates the significance of the risks posed by the draft decision as regards the fundamental rights and freedoms of data subjects and, where applicable, the free flow of personal data within the Union;
- **Information society service** means any service normally provided for remuneration, at a distance, by electronic means and at the individual request of a recipient of services;

All stakeholders are responsible for reporting known breaches internally to a senior manager or to the Data Protection Officer as soon as the breach is recognised. The responsible member of the senior leadership team should be informed.

- **International Academy** means an Academy and its subordinate bodies governed by public international law, or any other body which is set up by, or on the basis of, an agreement between two or more countries;

- **Special categories** of personal data means personal data:

    - revealing racial or ethnic origin;
    - revealing political opinions;
    - revealing religious or philosophical beliefs or trade union membership;
    - the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person;
    - data concerning health or data concerning a natural person's sex life or sexual orientation;

- **Data breach** an incident or event in which personal and/or confidential data:

    - has potentially been viewed or used by an individual unauthorised to do so;
    - has had its integrity compromised;
    - is lost or is unavailable for a significant period.

All stakeholders are responsible for reporting known breaches internally to a senior manager or to the Data Protection Officer as soon as the breach is recognised. The responsible member of the senior leadership team should be informed.

APPENDIX 2 - EXAMPLES OF DATA BREACHES

- Loss or theft of paper records or loss or theft of equipment on which data is stored e.g. a laptop, mobile phone, tablet device or memory stick;
- A letter or email containing personal and/or confidential data sent to the wrong address (including internal staff or third parties} or an email to an unauthorised group of email boxes;
- Personal data disclosed orally in error in a meeting or over the phone - including "blogging" where information is obtained by deceiving the Academy, or where information has been disclosed without confirming the true identity of the requester;
- Unauthorised access to information classified as personal or confidential e.g. attaching documents to an outlook diary appointment that is openly accessible;
- Posting information on the world wide web or on a computer otherwise accessible from the Internet without proper information security precautions;
- Sensitive information left on a photocopier or on a desk in the premises;
- Unauthorised alteration or deletion of information;
- Not storing personal and confidential information securely;
- Not ensuring the proper transfer or destruction of files after closure of offices/buildings e.g. not following building decommissioning procedures;
- Failure to safeguard/remove personal data on office equipment (including computers and smartphones} before disposal/sale.

Examples of Breaches caused by IT Security Incidents

- Unauthorised access to IT systems because of misconfigured and/or inappropriate access controls;
- Hacking or phishing attacks and related suspicious activity;
- Virus or malware attacks and related suspicious activity;
- ICT infrastructure-generated suspicious activity;
- Divulging a password to another user without authority.

All stakeholders are responsible for reporting known breaches internally to a senior manager or to the Data Protection Officer as soon as the breach is recognised. The responsible member of the senior leadership team should be informed.

All stakeholders are responsible for reporting known breaches internally to a senior manager or to the Data Protection Officer as soon as the breach is recognised. The responsible member of the senior leadership team should be informed.

APPENDIX 3 - DEALING WITH SUBJECT ACCESS REQUESTS

What must the Academy do?	Why?	How?
We must be clear about the nature of the request and identify what information is being requested.	Being clear about the nature of the request will enable you to decide whether the request needs to be dealt with in accordance with statutory requirements, who needs to deal with the request, and/or whether this is business as usual (BAU). If needed ask the submitter of the request for clarity.	Review the request and identify: If the request is for the personal information of the requester or made by an individual on behalf of another person (e.g. on behalf of a child or an adult lacking capacity) - this is a subject access request; If the request is for non- personal information - this may be dealt with as BAU or formally under the Freedom of Information Act 2000 (the FOIA) or the Environmental Information Regulations 2004 (the EIR). **NB:** The request can be received in a range of different formats e.g. letter, email, a completed form, or can be made via social media (e.g. a Facebook page or Twitter account).

All stakeholders are responsible for reporting known breaches internally to a senior manager or to the Data Protection Officer as soon as the breach is recognised. The responsible member of the senior leadership team should be informed.

If the request is a SAR the request must be forwarded to the responsible member of staff (usually the Principal) and the DPO within two working days of receipt of the request.	The GDPR stipulates that SARs must be completed within one month of the request - but in reality, as soon as possible.	Log the SAR in the subject access request log and inform all appropriate staff required to deal with the request.
If the information requested is for non-personal information i.e. is it Academy or statistical information, this will fall under the FOIA or EIR, or BAU and will be dealt with, as follows: All non-routine FOIA or EIR requests must be forwarded to the responsible member of staff (usually the Principal) and the DPO within two working days of receipt of the request.	The FOIA and EIR stipulates that requests must be completed within 20 working days of the request - therefore the more swiftly requests are being dealt with, the more likely the Academy will meet its statutory deadlines. BAU requests need to be dealt with by an individual in that particular service area who can identify and locate the information requested and provide a response within a reasonable timeframe.	If the request is for non-routine/FOIA/EIR information contact the responsible member of staff (usually the Principal) and the DPO.
If the information requested is for the personal information of an individual for use in a criminal investigation by the police, or any other agency	It is in the public interest that requests are identified and dealt with as quickly as possible.	Scan and email the request to the responsible member of staff (usually the Principal) and the DPO as needed.

All stakeholders are responsible for reporting known breaches internally to a senior manager or to the Data Protection Officer as soon as the breach is recognised. The responsible member of the senior leadership team should be informed.

investigating criminal offences, this will fall under either the regulatory Investigative Powers Act 2000 (RIPA) or Data Protection Act 2018. The request can be for either hard copy or any type of electronic information including email traffic i.e. the time and information that an email is sent. The request must be forwarded to the responsible member of staff (usually the Principal) and the DPO within two days.		