General Data Protection Regulation Policy

2021-2023

Version: **Date: June 2021**	
Ratified by the Board of Trustees, Finance, Audit, Risk & Personnel Committee	
Signed by the Board of Trustees, Finance, Audit, Risk & Personnel Committee	**Date: 21.06.2021**
To be reviewed every 2 years	**Date: 21.06.2023**

Contents

1. Introduction

1.1. The board of Trustees are committed to conducting its business in accordance with all applicable Data Protection laws and regulations and in line with the highest standards of ethical conduct.

1.2. This policy details expected behaviours o Academy's Employees and third parties in relation to the collection, use, retention, transfer, disclosure and destruction of any Personal Data belonging to a pupil, parent or staff member of the Academy and irrespective of the media used to store the information.

2. Definitions

2.1. Personal Data is any information (including opinions and intentions) which relates to an identified or Identifiable Natural Person. Personal Data is subject to certain legal safeguards and other regulations, which impose restrictions on how organisations may process Personal Data.

2.2. An organisation that handles personal data and makes decisions about its use is known as a Data Controller. The Academies, as Data Controllers, are responsible for ensuring compliance with the Data Protection requirements outlined in this policy.

2.3. Non-compliance may expose the Trust to complaints, regulatory action, fines and/or reputational damage.

2.4. The board of Trustees are fully committed to ensuring continued and effective implementation of this policy and expects all Academy employees and third parties to share in this commitment.

2.5. Any breach of this policy will be taken seriously and may result in disciplinary action.

2.6. The academies have notified the Information Commissioner's Officer of its data processing and its registration number as follows: ZB037371

3. Scope

3.1. This policy applies to all activities undertaken by the Trust where a Data Subject's personal data is processed in the context of the general educational activities of the school/MAT.

3.2. This policy applies to all processing of personal data in electronic form (including electronic mail and documents created with word processing software) or where it is held in manual files that are structured in a way that allows ready access to information about individuals.

3.3. This policy has been designed to establish a baseline standard for the processing and protection of personal data by all Trust Employees. Where national law imposes a requirement that is stricter than that imposed by this policy, the requirements in national law must be followed. Furthermore, where national law imposes a requirement that is not addressed in this policy, the relevant national law must be adhered to.

3.4. The protection of personal data belonging to Academy employees is not within the scope of this policy.

3.5. The Data Champion for the Trust is responsible for overseeing this policy and, as applicable, developing related policies and privacy guidelines. The Data Champion within the Trust is Zoe Allcott z.allcott@thrive.ac 0121 7262853

3.6. Please contact the Data Champion or our DPO, with any questions about the operation of this policy or if you have any concerns that this policy is not being, or has not been, followed. In particular, you must always contact the DPO in the following circumstances:

- if you are unsure of the lawful basis which you are relying on to process Personal Data (including the legitimate interests used by the school)
- if you need to rely on Consent and/or need to capture Explicit Consent
- if you need to draft Privacy Notices or Fair Processing Notices
- if you are unsure about the retention period for the Personal Data being processed
- if you are unsure about what security or other measures you need to implement to protect Personal Data
- if there has been a Personal Data breach
- if you are unsure on what basis to transfer Personal Data outside the EEA (European Economic Area)
- if you need any assistance dealing with any rights invoked by a Data Subject
- whenever you are engaging in a significant new, or change in, processing activity which is likely to require a DPIA (Data Protection Impact Assessment) or plan to use Personal Data for purposes other than what it was collected for

- if you plan to undertake any activities involving automated processing including profiling or automated decision-making
- if you need help complying with applicable law when carrying out direct marketing activities; or
- if you need help with any contracts or other areas in relation to sharing Personal Data with third parties.

3.7. The Data protection officer for the Trust is as follows:

Data Protection Officer: Judicium Consulting Limited

Address: 72 Cannon Street, London, EC4N 6AE

Email: dataservices@judicium.com

Web: www.judiciumeducation.co.uk

Telephone: 0203 326 9174

Lead Contact: Craig Stilwell

4. Definitions

TERM	DEFINITION
ANONYMISATION	Data amended in such a way that no individuals can be identified from the data (whether directly or indirectly) by any means or by any person.
BINDING CORPORATE RULES	The Personal Data protection policies used for the transfer of Personal Data to one or more Third Countries within a group of undertakings, or group of enterprises engaged in a joint economic activity.
CONSENT	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.
CUSTOMER	Any past, current or prospective Kingsbury Academy customer.

DATA CONTROLLER	A 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.
DATA PROCESSOR	A natural or legal person, Public Authority, Agency or other body which Processes Personal Data on behalf of a Data Controller.
DATA PROTECTION	The process of safeguarding Personal Data from unauthorised or unlawful disclosure, access, alteration, Processing, transfer or destruction.
DATA PROTECTION OFFICER (DPO)	The person required to be appointed in specific circumstances under the GDPR. Where a mandatory DPO has not been appointed, this term means a data protection manager or other voluntary appointment of a DPO or refers to the Company data privacy team with responsibility for data protection compliance.
DATA SUBJECT	Anyone 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 one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.
EEA	The 28 countries in the EU, and Iceland, Liechtenstein and Norway.
EMPLOYEE	An individual who works part-time or full-time for Kingsbury Academy under a contract of employment, whether oral or written, express or implied, and has recognised rights and duties – includes temporary employees and independent contractors.
ENCRYPTION	The process of encoding a message or information in such a way that only authorised parties can access it.

INFORMATION COMMISSIONER'S OFFICE (ICO)	An independent Public Authority in the UK responsible for monitoring the application of the relevant Data Protection regulation set forth in national law.
PERSONAL DATA BREACH	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.
PROCESS, PROCESSED, PROCESSING	Any operation or set of operations performed on Personal Data or on sets of Personal Data, whether or not by automated means. Operations performed may include collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.
PROFILING	Any form of automated processing of Personal Data, where Personal Data is used to evaluate specific or general characteristics relating to a data subject. In particular to analyse or predict certain aspects concerning that natural person's performance at work, economic situations, health, personal preferences, interests, reliability, behaviour, location or movement.
PSEUDONYMISATION	Data amended in such a way that no individuals can be identified from the data (whether directly or indirectly) without a 'key' that allows the data to be re-identified.
SPECIAL CATEGORIES OF DATA	Personal Data pertaining to or revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, data concerning health or sex life and sexual orientation, genetic data or biometric data.

5. Governance Roles and Responsibilities

5.1. Policy Dissemination and Enforcement

5.1.1. The board of Trustees must ensure that all its employees responsible for the processing of personal data are aware of, and comply with, the contents of this policy. In addition, the Academies will make sure all third parties engaged to process personal data on their behalf (i.e. their Data Processors) are aware of, and comply with, the contents of this policy. Assurance of such compliance must be obtained from all third parties, whether companies or individuals, prior to granting them access to personal data controlled by the Academies.

5.2. Data Protection by Design & Default

5.2.1. The Academies must ensure that a Data Protection Impact Assessment (DPIA) is conducted for all new and/or revised systems or processes for which it has responsibility where the system or process stores personal data. The Data Champion shall advise on how to conduct the DPIA. The subsequent findings of the DPIA must then be submitted to the Data Protection Officer for review and approval. Where applicable, the Information Technology (IT) department, as part of its IT system and application design review process, will cooperate with the Data Protection subject matter expert to assess the impact of any new technology uses on the security of Personal Data.

5.3. Compliance Monitoring

5.3.1. To confirm that an adequate level of compliance is being achieved by the board of Trustees in relation to this policy, the Academies will carry out annual Data Protection compliance audits. Each audit will, as a minimum, assess compliance with this policy and the operational practices in relation to the protection of Personal Data, including:

- the assignment of responsibilities
- raising awareness
- training of Employees
- adequacy of organisational and technical controls to protect Personal Data
- records management procedures (including data minimisation)
- adherence to the qualified rights of the Data Subject
- Privacy by Design and Default
- consent for direct marketing

- Personal Data transfers
- Personal Data incident management (including Personal Data breaches)
- Personal Data complaints handling
- the currency of Data Protection policies and Privacy Notices
- the accuracy of Personal Data being stored
- the conformity of Data Processor activities
- the adequacy of procedures for redressing poor compliance.

5.3.2. Any major deficiencies identified will be reported to and monitored by the Trustees.

6. Data Protection Principles

6.1. Data Protection

6.1.1. The Academies have adopted the following principles to govern its collection, use, retention, transfer, disclosure and destruction of Personal Data.

PRINCIPLE	DEFINITION
PRINCIPLE 1: Lawfulness, Fairness and Transparency	Personal data shall be processed lawfully, fairly and in a transparent manner in relation to the data subject. This means the Academies must tell the Data Subject what processing will occur (transparency), the processing must match the description given to the Data Subject (fairness), and it must be for one of the purposes specified in the applicable Data Protection regulation (lawfulness).
PRINCIPLE 2: Purpose Limitation	Personal Data shall be collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes. This means the Academies must specify exactly what the personal data collected will be used for and limit the processing of that personal data to only what is necessary to meet the specified purpose.
PRINCIPLE 3: Data Minimisation	Personal data shall be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed. This means the Academies must not store any personal data beyond what is strictly required.
PRINCIPLE 4: Accuracy	Personal data shall be accurate and kept up to date. This means the Academies must have in place processes for

	identifying and addressing out-of-date, incorrect and redundant personal data.
PRINCIPLE 5: Storage Limitation	Personal data shall be kept in a form which permits identification of Data Subjects for no longer than is necessary for the purposes for which the personal data is processed. This means the Academies must, wherever possible, store personal data in a way that limits or prevents identification of the Data Subject.
PRINCIPLE 6: Integrity & Confidentiality	Personal data shall be processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing, and against accidental loss, destruction or damage. The Academies must use appropriate technical and organisational measures to ensure the integrity and confidentiality of personal data are maintained at all times.

6.2. Accountability

6.2.1. The Data Controller shall be responsible for, and be able to demonstrate, compliance. This means the Academies must demonstrate that the six Data Protection Principles (outlined above) are met for all Personal Data for which it is responsible.

6.3. Data Collection

6.3.1. Personal Data should be collected only from the [Data Subject/parent/carer of the Data Subject] unless one of the following applies:

- The nature of the business purpose necessitates collection of the Personal Data from other persons or bodies.
- The collection must be carried out under emergency circumstances in order to protect the vital interests of the Data Subject or to prevent serious loss or injury to another person.
- If Personal Data is collected from someone other than the Data Subject, the Data Subject must be informed of the collection unless one of the following apply:
- the Data Subject has received the required information by other means
- the information must remain confidential due to a professional secrecy obligation
- a national law expressly provides for the collection, Processing, or transfer of the Personal Data.

6.3.2. Where it has been determined that notification to a Data Subject is required, notification should occur promptly, but in no case later than:

- one calendar month from the first collection or recording of the Personal Data
- at the time of first communication, if used for communication with the Data Subject
- at the time of disclosure, if disclosed to another recipient

6.4. Data Subject Consent

6.4.1. The Academies will obtain Personal Data only by lawful and fair means and, where appropriate, with the knowledge and consent of the individual concerned.

6.4.2. Academies shall establish a system for obtaining and documenting Data Subject consent for the collection, processing, and/or transfer of their personal data. The system must include provisions for:

- ensuring the request for consent is presented in a manner which is clearly distinguishable from any other matters
- ensuring the request for consent is made in an intelligible and easily accessible form, and uses clear and plain language
- ensuring the consent is freely given
- documenting the date, method and content of the disclosures made, as well as the validity, scope, and volition of the Consents given
- providing a simple method for a Data Subject to withdraw their consent at any time.

6.4.3. External Privacy Notes

6.4.4. The Academies website will include an online 'Privacy Notice' and an online 'Cookie Notice' fulfilling the requirements of applicable law.

7. Data Use

7.1. Data Processing Collecting Personal Data

7.1.1. Academies will process personal data in accordance with data protection regulations and applicable contractual obligations and will not process personal data unless at least one of the following requirements are met:

- The Data Subject has given consent to the processing of their personal data for a specific purpose.
- Processing of the personal data 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 Data Controller is subject.
- 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 Data Controller.
- Processing is necessary for the purposes of the legitimate interests pursued by the Data Controller or by a third party (except where such interests are overridden by the interests or fundamental rights and freedoms of the Data Subject, in particular where the Data Subject is a child).

7.2. CCTV

7.2.1. 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.

7.2.2. 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.

7.2.3. Any enquiries about the CCTV system should be directed to the Office Manager.

7.3. Special Categories of Personal Data

- Special categories of personal data include the following:
- racial or ethnic origin
- health-physical or mental
- political opinions
- religious or philosophical beliefs
- trade union membership
- data concerning sex life or sexual orientation

- genetic data
- biometric data, where processed in a manner that will uniquely identify a person.

7.3.2. Academies will only process sensitive personal data where the Data Subject expressly consents to such processing or where, for example, one of the following conditions apply:

- the processing is necessary for the Academies to discharge its legal duty
- the processing is specifically authorised or required by law
- the processing is necessary to protect the vital interests of the Data Subject or of another natural person where the Data Subject is physically or legally incapable of giving consent.

7.3.3. Where sensitive personal data is being processed, Academies will adopt additional protection measures.

7.4. Data Quality

7.4.1. Academies will adopt all necessary measures to ensure that the personal data it collects and processes is complete and accurate in the first instance and is updated to reflect the current situation of the Data Subject.

7.4.2. The measures adopted to ensure data quality include:

- correcting personal data known to be incorrect, inaccurate, incomplete, ambiguous, misleading or outdated, even if the Data Subject does not request rectification
- keeping personal data only for the period necessary, to satisfy the permitted uses or applicable statutory retention period
- the removal of personal data if in violation of any of the Data Protection principles or if the personal data is no longer required
- restriction, rather than deletion of personal data, insofar as:
- a law prohibits erasure
- erasure would impair legitimate interests of the Data Subject
- the Data Subject disputes that their Personal Data is correct and it cannot be clearly ascertained whether their information is correct or incorrect.

7.5. Direct Marketing

7.5.1. As a general rule, we will not send promotional or direct marketing material to parents, pupils, staff or stakeholders through digital channels such as mobile phones, email and the Internet, without first obtaining their consent.

7.5.2. The GDPR and Privacy and Electronic Communications (which governs Direct Marketing Activities within the EU) imports the GDPR standard for

- The consent must be freely given, specific, informed and unambiguous.
- The consent must be expressed by a statement or clear affirmative action. Silence, pre-ticked boxes or inactivity should therefore not constitute consent.
- The consent must be as easy to withdraw as it was to provide consent in the first place.
- The organisation must be able to demonstrate that the individual has consented.
- The consent language must be intelligible and use clear and plain language.

7.5.3. Contacting recipients via email to establish whether consent is in place also constitutes direct marketing and is prohibited without first obtaining consent from the Customer. The request for consent must be clearly distinguished from other matters. Prior consent, before sending electronic communications for direct marketing purposes will be required. This would mean if the Academies were proposing to email parents or prospective donors of financial or material donations, they would have to obtain prior consent.

7.5.4. Where personal data of pupils, including photographs, is used for digital marketing purposes such as an online prospectus and school/Trust website, the Data Subject must be informed at the point of initial contact that they have the right to object, at any stage, to having their data processed for such purposes. Where an objection is made all marketing-related processing of the personal data shall cease immediately and details will be kept on a suppression list with a record of the decision.

7.6. Data Retention Disposal of Records

7.6.1. To ensure fair processing, personal data will not be retained by the Academies for longer than necessary in relation to the purposes for which it was originally collected, or for which it was further processed.

7.6.2. The length of time for which the Academies needs to retain personal data is set out in the Academy 'Personal Data Retention Schedule'. This considers the legal and contractual requirements, both minimum and maximum, that influence the retention periods. All personal data should be securely deleted or destroyed as soon as possible where it has been confirmed that there is no longer a need to retain it.

7.7. Data Protection

7.7.1. The Academies will adopt physical, technical, and organisational measures to ensure the security and protect the confidentiality, integrity and availability of the 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 authorised users are able to access the Personal Data when they need it for authorised purposes

7.7.2. This includes the prevention of loss or damage, unauthorised alteration, access or Processing, and other risks to which it may be exposed by virtue of human action or the physical or natural environment.

7.8. Data Security

7.8.1. A summary of the personal data related security measures is provided below:

- Prevent unauthorised persons from gaining access to data processing systems in which personal data is processed.
- Prevent persons entitled to use a data processing system from accessing personal data beyond their needs and authorisations.
- Ensure that personal data in the course of electronic transmission during transport cannot be read or copied
- Ensure that access logs are in place to establish whether, and by whom, the personal data was entered, modified or removed from a data processing system.
- Ensure that in the case where processing is carried out by a Data Processor, the data can be processed only in accordance with the instructions of the Data Controller.

8. Data Subject Rights - Rights of the Individual

8.1. The process for attending to the following Data Subject rights is outlined in the Data Subject Access Policy:

- information access (SAR)
- objection to Processing.
- objection to automated decision-making and Profiling
- restriction of Processing
- data portability
- data rectification
- data erasure.

8.2. No administration fee will be charged for considering and/or complying with such a request unless the request is deemed to be unfounded or excessive in nature.

9. SAR's

9.1. Data Subjects are entitled to, based upon a request made and upon successful verification of their identity, the following information about their own personal data:

- the purposes of the collection, processing, use and storage of their personal data
- the source(s) of the personal data, if it was not obtained from the Data Subject
- the categories of personal data stored for the Data Subject
- the recipients, or categories of recipients, to whom the personal data has been or may be transmitted, along with the location of those recipients
- the envisaged period of storage for the personal data or the rationale for determining the storage period
- the retention periods applied to the data
- a summary of the security measures in place to protect the data
- request to erase personal data, if it is no longer necessary in relation to the purposes for which it was collected or processed, or to rectify inaccurate data or to complete incomplete data.

9.2. A response to each request will be provided within 1 calendar month of the **receipt** of the written request from the Data Subject. That period may be extended by two further months where necessary, considering the complexity and number of the requests.

9.3. Appropriate verification must confirm that the requestor is the Data Subject or their authorised legal representative. Data Subjects shall have the right to require the Academy to correct or supplement erroneous, misleading, outdated, or incomplete personal data.

9.4. Please refer to the Individuals Rights Policy for detailed guidance and procedures for responding to such requests.

10. Third-Party Data

10.1. It should be noted that situations may arise where providing the information requested by a Data Subject would disclose personal data about another individual. In such cases, information must be redacted or withheld as may be necessary or appropriate to protect that person's rights.

10.2. When personal data is collected indirectly (for example, from a third party or publicly available source), the Academy will provide the Data Subject with all the information required by the GDPR as soon as possible after collecting/receiving the data. The Academy will also check that the personal data was collected by the third party in accordance with the GDPR and on a basis which contemplates proposed processing of that personal data.

11. Law Enforcement Requests and Disclosures

11.1. Sharing Personal Data

11.1.1. In certain circumstances, it is permitted that Personal Data be shared without the knowledge or consent of a Data Subject. This is the case where the disclosure of the personal data is necessary for any of the following purposes:

- the prevention or detection of crime.
- the apprehension or prosecution of offenders
- the assessment or collection of a tax or duty
- by order of a court or by any rule of law.
- Or if another legal reason applies and consent is not required.

12. Data Protection Training

12.1. All Academy employees and employees of Third Parties (Data Processors) that have access to personal data will have their responsibilities under this policy outlined to them as part of their staff induction training. In addition, Academies and Third Parties will provide regular Data Protection training and procedural guidance for their staff. The training and procedural guidance set forth will consist of, at a minimum, the following elements:

- the Data Protection Principles set forth above
- each Employee's duty to use and permit the use of personal data only by authorised persons and for authorised purposes
- the need for, and proper use of, the forms and procedures adopted to implement this policy
- the correct use of passwords, security and other access mechanisms
- the importance of limiting access to personal data, such as by using password protected screen savers and logging out when systems are not being attended by an authorised person
- securely storing manual files, printouts and electronic storage media
- information on how to detect a phishing email
- proper disposal of personal data by using secure shredding facilities
- any special risks associated when conducting educational activities or duties.

13. Data Transfer – Sharing Personal Data

13.1. Academies may transfer personal data to internal or Third-Party recipients located in another country where that country is recognised as having an adequate level of legal protection for the rights and freedoms of the relevant Data Subjects.

13.2. Where transfers need to be made to countries lacking an adequate level of legal protection (i.e. Third Countries), they must be made in compliance with an approved transfer mechanism.

13.3. Academies may only transfer personal data where one of the six legal reasons (Consent, Contract, Public Task, Vital Interest, Legal Obligation, Legitimate Interest) listed below applies:

- the Data Subject has given Consent to the proposed transfer (Consent).

- the transfer is necessary for the performance of a contract with the Data Subject (Contract).
- the transfer is necessary for the implementation of pre-contractual measures taken in response to the Data Subject's request (Contract)
- the transfer is necessary for the conclusion or performance of a contract concluded with a Third Party in the interest of the Data Subject (Contract).
- the transfer is legally required on important public interest grounds (Public Task).
- the transfer is necessary for the establishment, exercise or defence of legal claims (Legal).

14. Transfers to Third Parties

14.1. Academies will only transfer personal data to, or allow access by, Third Parties when it is assured that the information will be processed legitimately and protected appropriately by the recipient. Where Third-Party processing takes place, Academies will first identify if, under applicable law, the Third Party is considered a Data Controller or a Data Processor of the Personal Data being transferred.

14.2. Where the Third Party is deemed to be a Data Controller, Academies will enter into an appropriate agreement with the Controller to clarify each party's responsibilities in respect to the personal data transferred.

14.3. Where the Third Party is deemed to be a Data Processor, Academies will enter into an adequate processing agreement with the Data Processor. The agreement must require the Data Processor to protect the personal data from further disclosure and to only process personal data in compliance with Academies instructions. In addition, the agreement will require the Data Processor to implement appropriate technical and organisational measures to protect the personal data, as well as procedures for providing notification of Personal Data Breaches.

14.4. When outsourcing services to a Third Party (including Cloud Computing services), Academies will identify whether the Third Party will process personal data on its behalf and whether the outsourcing will entail any Third Country transfers of Personal Data. Academies agrees to conduct Data Impact Assessments whenever a new process is implemented that presents a significant risk to pupil, parent or employee personal data and/or where a new digital system is implemented. Academies recognises that as a Data Controller, the decision to carry out a Data Impact Assessment lies with it. However, the implementation of a Data

Impact Assessments will be conducted with the guidance of the Trust's Data Protection Officer.

14.5. Regular audits of processing of personal data performed by Third Parties, especially in respect of technical and organisational measures they have in place, should be undertaken. Any major deficiencies identified will be reported to and monitored by the board of Trustees.

15. Complaints Handling

15.1. Data Subjects with a complaint about the processing of their personal data should put forward the matter in writing. An investigation of the complaint will be carried out to the extent that is appropriate based on the merits of the specific case. Academies will inform the Data Subject of the progress and the outcome of the complaint within a reasonable period.

15.2. If the issue cannot be resolved through consultation with the Data Subject, then the Data Subject should be advised that they may, at their option, seek redress a complaint to the Information Commissioner's Office (ICO).

16. Breach Reporting – Personal Data Breaches

16.1. Any individual who suspects that a Personal Data Breach has occurred due to the theft or exposure of personal data must immediately notify the Data Champion providing a description of what occurred. Notification of the incident can be made via e-mail to z.allcott@thrive.ac. The Data Champion should update the internal breach log, including pertinent facts relating to the incident, effects and remedial actions taken.

16.2. All reported incidents will be investigated to confirm whether or not a Personal Data Breach has occurred. For severe Personal Data Breaches, the Academies must inform the ICO within 72 hours of becoming aware of the breach (through the Data Champion). Where there is a risk of damage to the Data Subject, the affected Data Subjects should be advised of the personal data breach.

16.3. If an individual (staff member, parent or student) believes that their data has been compromised they can send a complaint to the 'Data Controller' who will forward this on to the Data Protection Officer for guidance or they can send a complaint directly to the ICO:

Information Commissioner's Office

Wycliffe House,

Water Ln,

Wilmslow

SK9 5AF

Telephone: 0303 123 1113, Monday-Friday 9am-5pm.

16.4. Guidance can be found in the Incident Management Policy.

17. Policy Maintenance and Publication

17.1. This policy shall be available to all Employees through the Trust website and shared Policy drive. A hard copy will also be available in the Administration Office to facilitate classroom-based staff with limited PC access.

18. Changes

Description	Date	Page	Section
DPO name & address Trust wide	01.04.2021	5	3.7
Inclusion of Data Champion: Zoe Allcott	01.04.2021	20	12.1