The Societas Trust
Data Protection (GDPR) Policy

1. Introduction
2. Scope
3. Accountability
4. Responsibility and Commitment
5. Staff Responsibility
6. Keeping of Records
7. Personal Data
8. Data Protection Principles
9. Consent
10. Data Subjects Rights and Requests
11. The Lawful basis on which information is Processed
12. Automated Processing
13. The Data Protection Officer
14. Privacy Notices
15. Privacy by Design
16. Data Privacy Impact Assessment
17. The Management of Risk Associated with Processing of Personal Data
18. Retention of Records
19. Data Disposal
20. Data Security
21. Photographs and Video
22. Provision of Data to Children
23. Parents Rights
24. The Management of Data Breaches
25. Inter- relationship with other Trust Policies
26. Glossary – Explaining the language around Data Protection
27. Appendices

Reviewed and Agreed by the Directors' Resources Committee on 15 November 2018 – to be reviewed annually.

1. Introduction

The Societas Trust is committed to ensuring personal information is properly managed, ensuring compliance with the General Data Protection Regulation (GDPR) which came into force on 25 May 2018 replacing the Data Protection Act 1998 [DPA].

This document is a statement of the aims and principles of the Societas Trust for ensuring the confidentiality and security of sensitive information relating to pupils, parents, and staff both permanent and temporary, volunteers, trustees and governors, suppliers and other third parties. The Policy was approved by the Directors' Board on 6 July 2018 and is subject to ongoing review. All the academies which form part of the Trust are bound by this policy.

The **Data Subject** referred to in the document relates to any individual about whom any data is collected used and stored. It includes but is not limited to employees. The **Data Controller** refers the organization who is responsible for storing and controlling such information which is The Societas Trust and the Academies that form part of the Trust.

Processing of data involves any activity that involves the use of personal data. This includes but is not limited to: obtaining, recording or holding data or carrying out any operation or set of operations on that data such as organising, amending, retrieving, using, disclosing, erasing or destroying it. Processing also includes transmitting or transferring personal data to third parties.

2. Scope

The General Data Protection Regulation (GDPR) ensures a balance between an individual's rights to privacy and the lawful processing of personal data undertaken by organisations in the course of their business. It aims to protect the rights of individuals about whom data is obtained, stored, processed or supplied and requires that organisations take appropriate security measures against unauthorized access, alteration, disclosure or destruction of personal data.

Purpose and Categories of Individuals about whom information is processed

In order to operate efficiently The Societas Trust and the academies therein have to collect and use information about people with whom it works. These may include members of the public, current, past and prospective employees, governors, directors and members, pupils and parents, and suppliers, third party agencies. In addition it may be required by law to collect and use information in order to comply with the requirements of central government

We hold pupil data and use it for: -

- Pupil selection (and to confirm the identity of prospective pupils and their parents);
- Providing education services and extra-curricular activities to pupils, and monitoring pupils' progress and educational needs;
- Informing decisions such as the funding of schools;
- Assessing performance and to set targets for schools;
- Safeguarding pupils' welfare and providing appropriate pastoral (and where necessary medical) care;
- Support teaching and learning;

- Giving and receive information and references about past, current and prospective pupils, and to provide references to potential employers of past pupils;
- Managing internal policy and procedure;
- Enabling pupils to take part in assessments, to publish the results of examinations and to record pupil achievements;
- To carry out statistical analysis for diversity purposes;
- Legal and regulatory purposes (for example child protection, diversity monitoring and health and safety) and to comply with legal obligations and duties of care;
- Enabling relevant authorities to monitor the school's performance and to intervene or assist with incidents as appropriate;
- Monitoring use of the school's IT and communications systems in accordance with the school's IT security policy;
- Making use of photographic images of pupils in school publications, on the school website and on social media channels;
- Security purposes, including CCTV; and
- Where otherwise reasonably necessary for the school's purposes, including to obtain appropriate professional advice and insurance for the school.
- To provide support to pupils after they leave the school

We share pupil information with: -

- the Department for Education (DfE) - on a statutory basis under section 3 of The Education (Information About Individual Pupils) (England) Regulations 2013;
- Ofsted;
- Youth support services – under section 507B of the Education Act 1996, to enable them to provide information regarding training and careers as part of the education or training of 13-19 year olds;
- other schools within the Federation/Trust;
- Other Schools that pupils have attended/will attend;
- NHS;
- Welfare services (such as social services);
- Law enforcement officials such as police, HMRC;
- Local Authority Designated Officer;
- Professional advisors such as lawyers and consultants;
- Support services (including insurance, IT support, information security); and
- The Local Authority.

We collect and share information relating to Staff for the following reasons:

- contractual requirements – staff contract forms;
- employment checks, right to work;
- safeguarding and Safer Recruitment Requirements eg, Enhanced DBS Disclosures;
- salary requirements;
- legislative compliance;
- monitoring purposes;
- workforce planning/ Workforce Census;
- HR Administration and Processes.

We process personal data for employment purposes to assist in the running of the academy and to enable individuals to be paid. The collection of this information benefits both national and local users by:

- improving the management of workforce data across the sector;

- enabling development of a comprehensive picture of the workforce and how it is deployed;
- informing the development of recruitment and retention policies;
- allowing improved financial modelling and planning;
- enabling disability and ethnicity monitoring;
- supporting the work of the School Teachers' Review Body.

Information will be provided to those agencies securely or anonymized where possible.

This policy applies to all personal information created or held by the Societas Trust in whatever format (e.g. paper, electronic, email, microfiche, film) and however it is stored, (for example ICT system/database, shared drive filing structure, email, filing cabinet, shelving and personal filing drawers).

The GDPR does not apply to access to information about deceased individuals.

3. Accountability

The Trust is responsible and demonstrates accountability with the GDPR Legislation through the management structure and framework of policies and procedures which are regularly reviewed. We protect and maintain a balance between data protection rights in accordance with GDPR by implementing appropriate technical and organisational measures.

4. **Responsibilities and Commitment (See Appendix 1)**

The Societas Trust is committed to ensuring that all its staff are aware of GDPR Data Protection Policies, legal requirements and that adequate training is provided to them. The requirements are that knowledge of this policy are mandatory for all staff employed by the Societas Trust and any third party contracted to provide services within the Trust.

The GDPR Management Structure and Framework within the Societas Trust will comprise representation as follows: A GDPR Board Director, and within each Academy within the Trust there is a GDPR Link Governor on the Local Governing Board who has individual academy responsibility together with the Headteacher who is the Data Protection Representative at each academy. The Members and Directors have delegated overall responsibility for compliance with the GDPR to the Data Protection Officer, Jon Lovatt, CEO. The Trust has set up an Emergency Management Committee in the event of Breaches and a GDPR Steering Group who meet on a regular basis to deal with all GDPR Issues. The Terms of Reference for the Steering Group can be found as (Appendix 2)

5. Staff Responsibilities

The requirements of this policy are mandatory for all staff employed by the Trust and any third party contracted to provide services to the Trust

All staff who process or use personal information must ensure that they follow the Data Processing Requirements. The Trust will ensure that Staff have undergone a role specific data protection training programme.

In respect of employment information all staff are responsible for

- Checking that any information that they provide to the school in connection with their employment is accurate and up to date
- Informing the school of any changes to information that they have provided, e.g. change of address. The school cannot be held responsible for any errors unless the staff member has informed the school of such changes
- Handling all personal data (e.g. pupil attainment data) with reference to this policy.

This policy does not form part of any individual's term and conditions of employment with the school and is not intended to have a contractual effect. Changes to data protection legislation will be monitored and further amendments may be required to this policy in order to remain compliant with legal obligations.

All members of staff are required to familiarize themselves with its content and comply with the provisions contained in it. Breach of this policy will be treated as a disciplinary action under the Trust's disciplinary policy.

Employee Obligations

Employees may have access to the personal data of other members of staff, suppliers, parents or pupils of the School in the course of their employment or engagement. If so, the School expects those employees to help meet the School's data protection obligations to those individuals. Specifically, you must: -

- Only access the personal data that you have authority to access, and only for authorised purposes;
- Only allow others to access personal data if they have appropriate authorisation;
- Keep personal data secure (for example by complying with rules on access to school premises, computer access, password protection and secure file storage and destruction [Please refer to the School's Security Policy for further details about our security processes]);
- Not to remove personal data or devices containing personal data from the School premises unless appropriate security measures are in place (such as Pseudonymisation, encryption, password protection) to secure the information;
- Not to store personal information on local drives.

It is a criminal offence to knowingly or recklessly obtain or disclose information about an individual without legitimate cause. Relevant, confidential data should only be given to:

- other members of staff on a need to know basis;
- relevant Parents/Guardians;
- other authorities if it is necessary in the public interest, e.g. prevention of crime;
- Other authorities, such as the LA and academies to which a pupil may move, where there are legitimate requirements (DfEE leaflet 0015/2000 entitled "Pupil Records and Reports" issued in March 2000 covers Data Protection issues and how and what information should be transferred to other academies. DfES/0268/2002 provides further information).

The Academy should not disclose anything on a pupil's record which would be likely to cause serious harm to their physical or mental health or that of anyone else. Therefore, those who create such records should ensure that such information is separated from other records.

Where there is doubt or statutory requirements conflict advice should be obtained.

When giving information to an individual, particularly by telephone, it is most important that the individual's identity is verified. If in doubt, questions should be asked of the individual, to which only he/she is likely to know the answers. Information should not be provided to other parties, even if related. For example: in the case of divorced parents it is important that information regarding one party is not given to the other party to which he/she is not entitled.

All contractors who hold or collect personal data are responsible for their own compliance with the GDPR and must ensure that personal information is kept and processed in-line with the GDPR.

6. Recording Data Processing Activities

The School are required to keep full and accurate records of our data processing activities. These records are detailed within this policy and include: -

- The name and contact details of the School;
- The name and contact details of the Data Protection Officer;
- Descriptions of the types of personal data used;
- Description of the data subjects;
- Details of the School's processing activities and purposes;
- Details of any third party recipients of the personal data;
- Where personal data is stored;
- Retention periods; which are referred to in the Data Retention Policy and
- Security measures in place.

The Trust is/has undertaking/undertaken data mapping activities and audit to ensure confidentiality integrity of our systems.

7. Personal Data

Personal data
Personal data is any information relating to an individual where the individual can be identified (directly or indirectly) from that data alone or in combination with other identifiers we possess or can reasonably access. This includes special category data and pseudonymised personal data but excludes anonymous data or data that has had the identity of an individual permanently removed.

Personal data can be factual (for examples a name, email address, location or date of birth) or an opinion about that person's actions or behaviour.
Personal data will be stored either electronically or as part of a structured manual filing system in such a way that it can be retrieved automatically by reference to the individual or criteria relating to that individual.

Special Category Data
Previously termed "Sensitive Personal Data", Special Category Data is similar by definition and refers to data concerning an individual Data Subject's racial or ethnic origin, political or religious beliefs, trade union membership, physical and mental health, sexuality, biometric or genetic data and personal data relating to criminal offences and convictions.

8. Data Protection Principles
The School are responsible for and adhere to the principles relating to the processing of personal data as set out in the GDPR.

The principles the School must adhere to are: -

1. Personal data must be processed lawfully, fairly and in a transparent manner;
2. Personal data must be collected only for specified, explicit and legitimate purposes;
3. Personal data must be adequate, relevant and limited to what is necessary in relation to the purposes for which it is processed;
4. Personal data must be accurate and, where necessary, kept up to date;
5. Personal data must not be kept in a form which permits identification of data subjects for longer than is necessary for the purposes for which the data is processed; and
6. Personal data must be processed in a manner that ensures its security using appropriate technical and organisational measures to protect against unauthorised or unlawful processing and against accidental loss, destruction or damage.

Further details on each of the above principles is set out below.

Principle 1: Personal data must be processed lawfully, fairly and in a transparent manner
The School only collect, process and share personal data fairly and lawfully and for specified purposes. The School must have a specified purpose for processing personal data and special category of data as set out in the GDPR.
Before the processing starts for the first time we will review the purposes of the particular processing activity and select the most appropriate lawful basis for that processing. We will then regularly review those purposes whilst processing continues in order to satisfy ourselves that the processing is necessary for the purpose of the relevant lawful basis (i.e. that there is no other reasonable way to achieve that purpose).

Personal Data
The School may only process a data subject's personal data if one of the following fair processing conditions are met: -

- The data subject has given their consent;
- The processing is necessary for the performance of a contract with the data subject or for taking steps at their request to enter into a contract;
- To protect the data subject's vital interests;
- To meet our legal compliance obligations (other than a contractual obligation);
- To perform a task in the public interest or in order to carry out official functions as authorised by law;
- For the purposes of the School's legitimate interests where authorised in accordance with data protection legislation. This is provided that it would not prejudice the rights and freedoms or legitimate interests of the data subject.

Special Category Data
The School may only process special category data if they are entitled to process personal data (using one of the fair processing conditions above) AND one of the following conditions are met: -

- The data subject has given their explicit consent;
- The processing is necessary for the purposes of exercising or performing any right or obligation which is conferred or imposed on the School in the field of employment law, social security law or social protection law. This may include, but is not limited to, dealing with sickness absence, dealing with disability and making adjustments for the same, arranging private health care insurance and providing contractual sick pay;
- To protect the data subject's vital interests;
- To meet our legal compliance obligations (other than a contractual obligation);
- Where the data has been made public by the data subject;
- To perform a task in the substantial public interest or in order to carry out official functions as authorised by law;
- Where it is necessary for the purposes of preventive or occupational medicine, for the assessment of the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment or the management of health or social care systems and services;
- Where it is necessary for reasons of public interest in the area of public health;
- The processing in necessary for archiving, statistical or research purposes.

The School identifies and documents the legal grounds being relied upon for each processing activity.

Principle 2: Personal data must be collected only for specified, explicit and legitimate purposes
Personal data will not be processed in any matter that is incompatible with the legitimate purposes.
The School will not use personal data for new, different or incompatible purposes from that disclosed when it was first obtained unless we have informed the data subject of the new purpose (and they have consented where necessary).

Principle 3: Personal data must be adequate, relevant and limited to what is necessary in relation to the purposes for which it is processed
The School will only process personal data when our obligations and duties require us to. We will not collect excessive data and ensure any personal data collected is adequate and relevant for the intended purposes.
When personal data is no longer needed for specified purposes, the School shall delete or anonymise the data. [Please refer to the School's Data Retention Policy for further guidance].

Principle 4: Personal data must be accurate and, where necessary, kept up to date
The School will endeavour to correct or delete any inaccurate data being processed by checking the accuracy of the personal data at the point of collection and at regular intervals afterwards. We will take all reasonable steps to destroy or amend inaccurate or out of date personal data.
Data subjects also have an obligation to ensure that their data is accurate, complete, up to date and relevant. Data subjects have the right to request rectification to incomplete or inaccurate data held by the School.

Principle 5: Personal data must not be kept in a form which permits identification of data subjects for longer than is necessary for the purposes for which the data is processed
Legitimate purposes for which the data is being processed may include satisfying legal, accounting or reporting requirements. The School will ensure that they adhere to legal timeframes for retaining data.
We will take reasonable steps to destroy or erase from our systems all personal data that we no longer require. We will also ensure that data subjects are informed of the period for which data is stored and how that period is determined in our privacy notices.
Please refer to the School's Retention Policy for further details about how the School retains and removes data.

Principle 6: Personal data must be processed in a manner that ensures its security using appropriate technical and organisational measures to protect against unauthorised or unlawful processing and against accidental loss, destruction or damage
In order to assure the protection of all data being processed, the School will develop, implement and maintain reasonable safeguard and security measures. This includes using measures such as: -

- Encryption;
- Pseudonymisation (this is where the School replaces information that directly or indirectly identifies an individual with one or more artificial identifiers or pseudonyms so that the person to whom the data relates cannot be identified without the use of additional information which is meant to be kept separately and secure);
- Ensuring authorised access (i.e. that only people who have a need to know the personal data are authorised to access it);
- Adhering to confidentiality principles;
- Ensuring personal data is accurate and suitable for the process for which it is processed.

The School follow procedures and technologies to ensure security and will regularly evaluate and test the effectiveness of those safeguards to ensure security in processing personal data. The School will only transfer personal data to third party service providers who agree to comply with the required policies and procedures and agree to put adequate measures in place.

Sharing Personal Data
The School will generally not share personal data with third parties unless certain safeguards and contractual arrangements have been put in place. These include if the third party: -

- Has a need to know the information for the purposes of providing the contracted services;
- Sharing the personal data complies with the privacy notice that has been provided to the data subject and, if required, the data subject's consent has been obtained;
- The third party has agreed to comply with the required data security standards, policies and procedures and put adequate security measures in place;
- The transfer complies with any applicable cross border transfer restrictions; and
- A fully executed written contract that contains GDPR approved third party clauses has been obtained.

There may be circumstances where the School is required either by law or in the best interests of our pupils, parents or staff to pass information onto external authorities, for example, the local authority, Ofsted or the department of health. These authorities are up to date with data

protection law and have their own policies relating to the protection of any data that they receive or collect.
The intention to share data relating to individuals to an organisation outside of our Trust shall be clearly defined within written notifications and details and basis for sharing that data given.

Transfer of Data Outside the European Economic Area (EEA)
The GDPR restricts data transfers to countries outside the EEA in order to ensure that the level of data protection afforded to individuals by the GDPR is not undermined.
The School will not transfer data to another country outside of the EEA without appropriate safeguards being in place and in compliance with the GDPR. All staff must comply with the School's guidelines on transferring data outside of the EEA. For the avoidance of doubt, a transfer of data to another country can occur when you transmit, send, view or access that data in that particular country.

9. Consent

Consent
Where the School relies on consent as a fair condition for processing (as set out above), it will adhere to the requirements set out in the GDPR.

Consent only needs to be obtained to process data when they cannot do so under any other lawful basis - See Section 11:

When obtaining, recording and managing consent, academies within the Trust will make sure:

- Their request for consent is specific about why they want the data, what they will do with the data, if the data will be outsourced to a third party, and that the data subject has the right to withdraw their consent at any time.
- The request for consent asks people to actively opt-in. A data subject will have consented to processing of their personal data if they indicate agreement clearly either by a statement or positive action to the processing. Consent requires affirmative action so silence, pre-ticked boxes or inactivity will not amount to valid consent
- Wherever possible, they give separate options for different purposes and different types of processing
- That records are kept to evidence consent, including who consented, when, how, and what they were told
- It is easy for the data subject to withdraw consent and how they can withdraw
- Consents obtained are kept under review to ensure that there is still a valid reason for processing within the specified timeframe
- Explicit consent requires a very clear and specific statement of what is being consented to of how and why the data will be used.

If explicit consent is not required, the School will normally seek another legal basis to process that data. However if explicit consent is required the data subject will be provided with full information in order to provide explicit consent.
If any of the processes or processing activities change after consent is obtained the school with obtain further consent.

The school will keep consent under review to ensure that it is still valid for the given time. I.e. during an academic year or until the child reaches an age when they are able to provide their

own consent.

Consent for Children
The GDPR does not prescribe an age at which a person is considered to be a child. The general rule is if the child had the competence to understand consent for themselves. Where the child is assessed to have this competence, then schools must ensure that any requests are written in easy to understand language

Young children such as children in primary school and the start of secondary school are not likely to have the competence to consent to the processing of their data so schools are likely to need consent from parents to process pupil data. Further guidance is being developed by the ICO.

The School will keep records of consents obtained in order to demonstrate compliance with consent requirements under the GDPR. Communication to parents is sent relating to consent (**Appendix 3)** and a Consent Template for each academy to use align to their specific process included**(Appendix 4)**

Right to Withdraw Consent
Data subjects must be easily able to withdraw consent to processing at any time and withdrawal must be promptly honoured. In circumstances where an individual may have provided consent to the collection, processing and transfer of personal information for a specific purpose, they have the right to withdraw consent for that specific processing at any time. To withdraw consent please contact the office manager of your academy. Once notification has been received that consent is withdrawn, information will be no longer processed in line with the purpose(s) you agreed to, unless we have another legitimate basis for doing so.

10. <u>Data Subject's Rights and Requests</u>
Personal data must be made available to data subjects as set out within this policy and data subjects must be allowed to exercise certain rights in relation to their personal data.
The rights data subjects have in relation to how the School handle their personal data are set out below: -

(a) Where consent is relied upon as a condition of processing) To withdraw consent to processing at any time;
(b) Receive certain information about the School's processing activities;
(c) Request access to their personal data that we hold
(d) Prevent use of their personal data for marketing purposes
(e) Ask us to erase personal data if it is no longer necessary in relation to the purposes for which was collected or processed or to rectify inaccurate data or to complete incomplete data
(f) Restrict processing in specific circumstances
(g) Challenge processing which has been justified on the basis of our legitimate interests or in the public interest
(h) Request a copy of an agreement under which personal data is transferred outside of the EEA
(i) Object to decisions bases solely on automated processing
(j) Prevent processing that is likely to cause damage or distress to the data subject or anyone else;
(k) Be notified of a personal data breach which is likely to result in high risk to their rights and freedoms;
(l) Make a complaint to the supervisory authority; and
(m) In limited circumstances, receive or ask for their personal data to be transferred to a third party in a structured, commonly used and machine readable format.

If any request is made to exercise the rights above, it is a requirement for the relevant staff member

within the School to verify the identity of the individual making the request.

Subject Access Requests (SAR)

A Data Subject has the right to be informed by the School of the following: -

(a) Confirmation that their data is being processed;
(b) Access to their personal data;
(c) A description of the information that is being processed;
(d) The purpose for which the information is being processed;
(e) The recipients/class of recipients to whom that information is or may be disclosed;
(f) Details of the School's sources of information obtained;
(g) In relation to any Personal Data processed for the purposes of evaluating matters in relation to the Data Subject that has constituted or is likely to constitute the sole basis for any decision significantly affecting him or her, to be informed of the logic of the Data Controller's decision making. Such data may include, but is not limited to, performance at work, creditworthiness, reliability and conduct.
(h) Other supplementary information

Any Data Subject who wishes to obtain the above information must notify the School in writing of his or her request. This is known as a Data Subject Access Request.
The request should in the first instance be sent to the Office Manager

11. The lawful basis on which we use information

We will only use your information when the law allows us to. Most commonly, we will use your information in the following circumstances: -

1. Consent of the data subject: the individual has given clear consent to process their personal data for a specific purpose;
2. Performance of a Contract: the processing is necessary for a contract with the individual;
3. Compliance with a Legal obligation: the processing is necessary to comply with the law (not including contractual obligations);
4. To Protect the Vital interests of a data subject or another person: the processing is necessary to protect someone's life.
5. Public task – in the Public interest: the processing is necessary to perform a task in the public interest or for official functions, and the task or function has a clear basis in law; and
6. Legitimate Interests: The Education Act 1996: for Departmental Censuses 3 times a year. More information can be found at: https://www.gov.uk/education/data-collection-and-censuses-for-schools.

We need all the categories of information in the list above primarily to allow us to comply with legal obligations. Please note that we may process information without knowledge or consent, where this is require or permitted by law.

12. Automated Processing

Any form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to an individual, in particular to analyse or predict aspects concerning that individual's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements.

Generally automated decision making is prohibited when a decision has a legal or similar significant

effect on an individual unless:

(a) The data subject has given explicit consent;

(b) The processing is authorised by law; or

(c) The processing is necessary for the performance of or entering into a contract.

If certain types of sensitive data are being processed, then (b) or (c) above will not be allowed unless it is necessary for the substantial public interest (for example fraud prevention).

If a decision is to be based solely on automated processing, then data subjects must be informed of their right to object. This right will be explicitly brought to their attention and presented clearly and separately from other information. Further, suitable measures must be put in place to safeguard the data subject's rights and freedoms and legitimate interests.

The School will also inform the data subject of the logic involved in the decision making or profiling, the significance and envisaged consequences and give the data subject the right to request human intervention, express their point of view or challenge the decision.

The school will carry out a data protection impact assessment before any automated processing or automated decision making activities are undertaken.

An example of automated processing includes profiling and automated decision making. Automatic decision making is when a decision is made which is based solely on automated processing which produces legal effects or significantly affects an individual. Automated decision making is prohibited except in exceptional circumstances

13. The Data Protection Officer

As a GDPR requirement the Trust has appointed J Lovatt CEO as the Data Protection Officer. ceo@societastrust.org.uk The Hub Office, Ellison Primary Academy, Ellison Street, Newcastle Under Lyme. Staffordshire ST5 0LB Tel 01782 613674

The DPO is responsible for overseeing this data protection policy and developing data-related policies and guidelines. Please contact the DPO with any questions about the operation of this Data Protection Policy or the GDPR 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: -

(a) If you are unsure of the lawful basis being relied on by the School to process personal data;
(b) If you need to rely on consent as a fair reason for processing (please see section (9) on consent for further detail);
(c) If you need to draft privacy notices or fair processing notices;
(d) If you are unsure about the retention periods for the personal data being processed;
(e) If you are unsure about what security measures need to be put in place to protect personal data;
(f) If there has been a personal data breach;
(g) If you are unsure on what basis to transfer personal data outside the EEA;
(h) If you need any assistance dealing with any rights invoked by a data subject;

(i) Whenever you are engaging in a significant new (or a change in) processing activity which is likely to require a data protection impact assessment or if you plan to use personal data for purposes other than what it was collected for;
(j) If you plan to undertake any activities involving automated processing or automated decision making;
(k) If you need help complying with applicable law when carrying out direct marketing activities;
(l) If you need help with any contracts or other areas in relation to sharing personal data with third parties.

Notification to the ICO

The GDPR requires every data controller who is processing personal data, to notify and renew their notification, on an annual basis. Failure to do so is a criminal offence. A copy of this notification is attached as Appendix.. The Information Commissioner maintains a public register of data controllers, in which the Academy is registered.
The Academy will review the Data Protection Register (http://www.ico.gov.uk/ESDWebPages/search.asp) annually, prior to renewing the notification to the Information Commissioner.

14. Privacy Notices

The School will provide detailed, specific information to data subjects. This information will be provided through the School's privacy notices which are concise, transparent, intelligible, easily accessible and in clear and plain language so that a data subject can easily understand them. Privacy notices sets out information for data subjects about how the School use their data and the School's privacy notices are tailored to suit the data subject.

Whenever we collect personal data directly from data subjects, including for human resources or employment purposes, we will provide the data subject with all the information required by the GDPR including the identity of the data protection officer, the School's contact details, how and why we will use, process, disclose, protect and retain personal data.

When personal data is collected indirectly (for example from a third party or publically available source), we will provide the data subject with the above information as soon as possible after receiving the data. The School will also confirm whether that third party has collected and processed data in accordance with the GDPR.

Notifications shall be in accordance with ICO guidance and, where relevant, be written in a form understandable by those defined as "children" under the GDPR

Privacy notices can be found at (Appendix 5 for Parents and Carers and Appendix 6 for Staff).

15. Privacy by Design

The School adopt a privacy be design approach to data protection to ensure that we adhere to data compliance and to implement technical and organisational measures in an effective manner.

Privacy by design is an approach that promotes privacy and data protection compliance from the start. To help us achieve this, the School takes into account the nature and purposes of the processing, any cost of implementation and any risks to rights and freedoms of data subjects when implementing data

processes. The Trust and academies therein undertake data mapping activities to identify the path of personal data through the processing and the relevant risks. A Pro Forma for a Data Map is illustrated in (Appendix 7)

16. Data Protection Impact Assessments (DPIAs)

In order to achieve a privacy by design approach, the School conduct DPIAs for any new technologies or programmes being used by the School which could affect the processing of personal data. In any event the School carries out DPIAs when required by the GDPR in the following circumstances: -

- For the use of new technologies (programs, systems or processes) or changing technologies;
- For the use of automated processing;
- For large scale processing of special category data;
- For large scale, systematic monitoring of a publicly accessible area (through the use of CCTV).

Please see DPIA Template (Appendix 8)
Our DPIAs contain: -

- A description of the processing, its purposes and any legitimate interests used;
- An assessment of the necessity and proportionality of the processing in relation to its purpose;
- An assessment of the risk to individuals;

17. The Management of Risk Associated with Processing of Personal Data

The Trust's policies and procedures have been written to ensure there are practices in place to minimize the following risks which would result in a Data Breach:) Please see Section 24 for Management of Data Breaches)

Please see Appendix 9 detailing the risk management process

The Key Risks

a) unauthorized disclosure (Confidentiality) – unlawful or accidental disclosure of or access to personal data
b) Unauthorised Access -Availability breach – where there is an accidental or unauthorised loss of access to, or destruction of personal data.
c) Alteration - Integrity breach – where there is an unauthorised or accidental alteration of personal data

Examples of a data breach could include the following (but are not exhaustive): -

- Loss or theft of data or equipment on which data is stored, for example loss of a laptop or a paper file (this includes accidental loss);
- Inappropriate access controls allowing unauthorised disclosure or use;
- Equipment failure;
- Human error (for example sending an email or SMS to the wrong recipient);
- Unforeseen circumstances such as a fire or flood;
- Hacking, phishing and other "blagging" attacks where information is obtained by deceiving whoever holds it.

- Damage to where personal data has been altered, corrupted or no longer complete.

Assessing the Risk

Data Breaches or non-compliance with the GDPR would impact the Academy/Trust in a number of ways:

- Monetary
- Legislative
- Reputational
- It could personally impact the pupils staff and stakeholders
- Operational - -how long would it take to recover

Impact Level	
0	No impact on end user
1	Minor contact information compromised
2	Bulk contact information compromised – minimal impact to rights and freedoms but large reputational damage
3	Bulk contact financial information compromised – major impact to rights and freedoms and large reputational damage leading to failure of the organsation

We measure the risks in terms of the impact against the likelihood of the incident occurring and apply a scoring system to establish whether the risk is low, medium or high identifying what areas for prioritisation:

Likelihood	3	0	3	6	9
	2	0	2	4	6
	1	0	1	2	3
	0	0	1	2	3
	Impact				

We have considered the risk, the impact, the likelihood of occurrence against the cost and effort in implementing corrective measures.

Appetite for Risk

Risk Level	From	To	GDPR	Description of Risk Level
High	**6**	**9**	**High Risk**	**This risk exceeds the organisation's appetite**
Medium	**3**	**5**	**Unacceptable Risk**	**This risk could exceed the risk appetite under certain conditions**
Low	**1**	**2**	**Acceptable Risk**	**This risk is in acceptable boundaries**
Zero	**0**	**0**	**No Risk**	

Treatment of Risk
Terminate - the risk is high and exceeds the organisation's appetite – the organization will not proceed with the activities/processes
Tolerate – the risk has acceptable boundaries, it may not be cost effective to mitigate the risk, and the impact is low -
Transfer – the risk to another organization/contractor who are better able to carry the risk
Treat - take cost effective actions to reduce the risk moving it from high to medium or medium to low level

18. Retention Periods

Except as otherwise permitted or required by applicable law or regulation, the School only retains personal data for as long as necessary to fulfil the purposes they collected it for, as required to satisfy any legal, accounting or reporting obligations, or as necessary to resolve disputes.

To determine the appropriate retention period for personal data, the School considers the amount, nature, and sensitivity of personal data, the potential risk of harm from unauthorised use or disclosure of personal data, the purposes for processing the personal data, whether we can fulfil the purposes of processing by other means and any applicable legal requirements.

Once you are no longer an employee, worker or contractor of the company we will retain and securely destroy your personal information in accordance with our data retention policy.

The School typically retains personal data for 6 years subject to any exceptional circumstances or to comply with laws or regulations that require a specific retention period.

Please refer to the Trust Data Retention Policy

19. Data Disposal

The Trust recognized that the secure disposal of redundant data is an integral element to compliance with legal requirements and an area of increased risk. All data held in any form of media (paper, tape, electronic) shall only be passed to a disposal partner with demonstrable competence in providing secure disposal services and compliance with the requirements of the GDPR
All data shall be destroyed or eradicated to agreed levels meeting recognized national standards with confirmation at completion of disposal process

20. Data Security (Cross Reference to E Safety Policy) Update with Evolv Policy

The Trust recognize the importance of Confidentiality, Integrity and Availability of Data. We have implemented data security in our ICT systems ensuring that all staff are aware the responsibility of information security is applicable to everyone. This Policy includes guidance on incident and breach reporting in the event of an IT Security incident. In order to assure the protection of all data being processed and inform decisions on processing activities, we shall undertake an assessment of the associated risks of proposed processing and equally the impact on an individual's privacy in holding data related to them. Risk and impact assessments shall be conducted in accordance with guidance given by the ICO

We have put in place proportionate physical and technical measures to protect the security of your information (i.e. against it being accidentally lost, used or accessed in an unauthorised way). These must be adhered to as follows:

- Ensured the use of a complex password system and staff have been advised against writing passwords down
- Academies are currently using encrypted USB Sticks and external hard drives with a view towards phasing them out.
- Work to be stored on appropriate School Drives which can be accessible from home using your designated teacher/staff laptop
- Laptops will be encrypted with appropriate software to ensure they are as secure as possible
- No pupil data or any confidential personal information should be stored on any home device.
- School email should be accessed on school servers so as not to compromise data. Emails should only be checked on encrypted school devices.
- Emails should not be synced to any phones or tablets
- Any files attached to emails to be password protected
- Printing/Copying from School Printers will now only be released from the printer by using your own unique staff printer codes
- Confidential data must not be left on screen when you leave your desk – your pc/laptop should be locked – so you will need to log back in
- Pupils have their own log in.
- Please be aware of the Staff Retention Schedule of what pupil data must be kept and ensure confidential documents are shredded where appropriate.
- Any Curriculum Software/Websites must have provided the Trust with a GDPR Compliance Statement (DCPro, Abacus, Purple Mash, Squid)

21. Photographs and video:

Images of staff and pupils may be captured at appropriate times and as part of education activities for

use in school only. Unless prior consent from parents/pupils/staff has been given, the school shall not utilize such images for publication or communication to external sources. It is the Trust's policy that external parties including parents may not capture images of pupils or staff during such activities without consent.

22 Provision of data to children

In relation to the capacity of a child to make a subject access request, guidance provided by the Information Commissioner's Office has been that by the age of 13 a child can be expected to have sufficient maturity to understand the nature of the request. A child may of course reach sufficient maturity earlier; each child should be judged on a case by case basis.

If the child does not understand the nature of the request, someone with parental responsibility for the child, or a guardian, is entitled to make the request on behalf of the child and receive a response.

Pupils who submit requests to access their educational records should be allowed to do so unless it is obvious that they do not understand what they are asking for.

23. Parents' rights

An adult with parental responsibility can access the information about their child, as long as the child is not considered to be sufficiently mature. They must be able to prove their parental responsibility and the academy is entitled to request relevant documentation to evidence this as well as the identity of the requestor and child.

In addition, parents have their own independent right under The Education (Pupil Information) (England) Regulations 2000 of access to the official education records of their children. Students do not have a right to prevent their parents from obtaining a copy of their academy records.

Any person whose details, or child's details, are to be included on the academy's website will be required to give written consent. At the time the information is included all such individuals will be properly informed about the consequences of their data being disseminated worldwide.

To obtain parents' permission for the use of photographs outside the academy and, in particular, to record their wishes if they do not want photographs to be taken of their children.

24. The Management of Data Breaches

The General Data Protection Regulation (GDPR) aims to protect the rights of individuals about whom data is obtained, stored, processed or supplied and requires that organisations take appropriate security measures against unauthorised access, alteration, disclosure or destruction of personal data.

The GDPR places obligations on staff to report actual or suspected data breaches and our procedure for dealing with breaches is set out below. All members of staff are required to familiarise themselves with its content and comply with the provisions contained in it. Training will be provided to all staff to enable them to carry out their obligations within this policy.

Data Processors will be provided with a copy of this policy and will be required to notify the School of any data breach without undue delay after becoming aware of the data breach. Failure to do so may result in a breach to the terms of the processing agreement.

Breach of this policy will be treated as a disciplinary offence which may result in disciplinary action under the School's Disciplinary Policy and Procedure up to and including summary dismissal depending on the seriousness of the breach.

This policy does not form part of any individual's terms and conditions of employment with the School and is not intended to have contractual effect. Changes to data protection legislation will be monitored and further amendments may be required to this policy in order to remain compliant with legal obligations.

What Is A Personal Data Breach?

The ICO defines a personal data breach as "a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data or special category data transmitted, stored or otherwise processed.
Breaches can be categorized as follows:

d) Confidentiality Breach – unlawful or accidental disclosure of or access to personal data
e) Availability breach – where there is an accidental or unauthorised loss of access to, or destruction of personal data.
f) Integrity breach – where there is an unauthorised or accidental alteration of personal data

Examples of a data breach could include the following (but are not exhaustive): -

- Loss or theft of data or equipment on which data is stored, for example loss of a laptop or a paper file (this includes accidental loss);
- Inappropriate access controls allowing unauthorised disclosure or use;
- Equipment failure;
- Human error (for example sending an email or SMS to the wrong recipient);
- Unforeseen circumstances such as a fire or flood;
- Hacking, phishing and other "blagging" attacks where information is obtained by deceiving whoever holds it.
- Damage to where personal data has been altered, corrupted or no longer complete.

When Does It Need To Be Reported?

The School must notify the ICO of a data breach where it is likely to result in a risk to the rights and freedoms of individuals. This means that the breach needs to be more than just losing personal data and if unaddressed the breach is likely to have a significant detrimental effect on individuals.

Examples of where the breach may have a significant effect includes: -

- potential or actual discrimination;
- potential or actual financial loss;
- potential or actual loss of confidentiality;
- risk to physical safety or reputation;
- exposure to identity theft (for example through the release of non-public identifiers such as passport details);
- the exposure of the private aspect of a person's life becoming known by others
- significant economic or social damage

If the breach is likely to result in a high risk to the rights and freedoms of individuals then the individuals must also be notified directly.

Reporting a Data Breach

If you know or suspect a personal data breach has occurred or may occur which meets the criteria above, you should: -

- Complete a data breach report form (which can be obtained from the Data Protection Representative at the Academy or from the Hub Manager or DPO Manager. (See Appendix 10)

A Breach Notification Form should contain the following information:

- The nature of the breach and the categories and approximate numbers of individuals concerned and the approximate number of records concerned
- The contact details of the person in the Academy who is dealing with the breach
- A description of the likely consequences of the Breach (If known)
- A description of the measures taken or proposed to be taken to deal with the breach
- What measures are to be taken to mitigate any possible adverse effects and repeat breaches

Breach reporting is encouraged throughout the Trust and staff are expected to seek advice if they are unsure as to whether the breach should be reported and/or could result in a risk to the rights and freedom of individuals. They can seek advice from their DPO Representative, The Hub Manager

or DPO.

Once reported, you should not take any further action in relation to the breach.

Managing and Recording The Breach

On being notified of a suspected personal data breach, the DPO will establish whether a personal data breach has in fact occurred. If so they will take steps to:-

- Where possible, contain the data breach;
- As far as possible, recover, rectify or delete the data that has been lost, damaged or disclosed;
- Assess and record the breach in the School's data breach register;
- Notify the ICO;
- Notify data subjects affected by the breach;
- Notify other appropriate parties to the breach;
- Take steps to prevent future breaches.

Notifying the ICO

The DPO will notify the ICO when a personal data breach has occurred which is likely to result in a risk to the rights and freedoms of individuals.

This will be done without undue delay and, where possible, within 72 hours of becoming aware of the breach. If all information is not to hand then information can be provided to the ICO in stages However, the initial investigation should begin as soon as possible and establish with a reasonable degree of certainty, whether a breach has taken place, and the consequences for individuals and the a more detailed investigation will follow. If the School are unsure of whether to report a breach, the assumption will be to report it.

Where the notification is not made within 72 hours of becoming aware of the breach, written reasons will be recorded as to why there was a delay in referring the matter to the ICO.

Notifying Data Subjects

Where the data breach is likely to result in a high risk to the rights and freedoms of data subjects, the DPO will notify the affected individuals without undue delay including the name and contact details of the DPO and ICO, the likely consequences of the data breach and the measures the School have (or intended) to take to address the breach.

When determining whether it is necessary to notify individuals directly of the breach, the DPO will co-operate with and seek guidance from the DPO, the ICO and any other relevant authorities (such as the police).

If it would involve disproportionate effort to notify the data subjects directly (for example, by not having contact details of the affected individual) then the School will consider alternative means to make those affected aware (for example by making a statement on the School website).

Notifying Other Authorities

The School will need to consider whether other parties need to be notified of the breach. For example:

- Insurers;
- Parents;
- Third parties (for example when they are also affected by the breach);
- Local authority;
- The police (for example if the breach involved theft of equipment or data).

This list is non-exhaustive.

Assessing the Breach

Once initial reporting procedures have been carried out, the School will carry out all necessary investigations into the breach.

The Academy Trust will identify how the breach occurred and take immediate steps to stop or minimise further loss, destruction or unauthorised disclosure of personal data. We will identify ways to recover correct or delete data (for example notifying our insurers or the police if the breach involves stolen hardware or data).

Having dealt with containing the breach, the School will consider the risks associated with the breach. These factors will help determine whether further steps need to be taken (for example notifying the ICO and/or data subjects as set out above). These factors include: -

- What type of data is involved and how sensitive it is;
- The volume of data affected;
- Who is affected by the breach (i.e. the categories and number of people involved);
- The likely consequences of the breach on affected data subjects following containment and whether further issues are likely to materialise;
- Are there any protections in place to secure the data (for example, encryption, password protection, pseudonymisation);
- What has happened to the data;
- What could the data tell a third party about the data subject;
- What are the likely consequences of the personal data breach on the school; and
- Any other wider consequences which may be applicable.

Preventing Future Breaches

Once the data breach has been dealt with, the School will consider its security processes with the aim of preventing further breaches. In order to do this, we will: -

- Establish what security measures were in place when the breach occurred;
- Assess whether technical or organisational measures can be implemented to prevent the breach happening again;
- Consider whether there is adequate staff awareness of security issues and look to fill any gaps through training or tailored advice;
- Consider whether it's necessary to conduct a privacy or data protection impact assessment;
- Consider whether further audits or data protection steps need to be taken;
- To update the data breach register;
- To debrief governors/management following the investigation.

Responsibility

In the event that there is a Data Breach, staff should report any potential breaches or concerns to their respective headteacher, who is the Data Processing Representative for the Academy, who in turn should report the matter direct to the Hub Manager, who will complete a Data Breach Form and submit to the DPO. DPO will review the Data Breach Forms to identify what corrective action may need to be implemented to prevent any further breaches.

25. Inter- relationship with other Trust Policies

- E Safety Policy
- Data Retention Policy
- Risk Management Register
- Information Security Policy
- Freedom of Information Policy
- Safeguarding Policy
- Social Networking Policy

26. Glossary – Explaining the language around Data Protection

Term	Description	Example
Data Subject	The individual who the data or information is about	John Smith the pupil or Jane Smith the teacher
Data Controller	The organization who (either alone or in common with other people) determine the purpose for which, and the manner in which data is processed A data controller is the individual or the legal person who controls and is responsible for the keeping and use of personal information on computer or in structured manual files.	The Trust and Academy is the Data Controller
Data Processor	A person or organization who process data on behalf of and on the orders of a controller	Staff, and a catering provider that the school may use
Data Item	A single piece of information about a data subject.	

Data Item Group	A group of data items that are typically captured about the same activity or business process in the academy. These are also sometimes called data elements or data scope within the data community/sharing agreements schools have with suppliers.	Attendance
Data Protection Impact Assessment (DPIA)	This is a process to consider the implication of some change you are introducing which may affect the privacy of individuals. Assessing privacy at the outset helps you plan consultation/awareness/consent type options from the outset. "Privacy by Design" involves the above process	
Data Breach	A personal data breach refers to a breach of security leading to the accidental or unlawful alteration, destruction, loss, or unauthorized Disclosure of and access to personal data. This includes breaches that are the result of accidental and deliberate. It also means that a breach is more than just about losing personal data.	
Data Retention	The amount of time the information is held for processing. At the end of the retention period, processes are in place to ensure it is properly disposed of.	
Data Audit/Data Asset Register	The assessment of data and its quality for a specific purpose. Other terms are data map or information asset register/log. This is the list of personal data assets that the holds and processes which may lead to adding further information	
Privacy Notice	This is a document that explains to the people you have data about (data subjects) what items you hold, what they are used for, who it is passed on to and why and what rights they have	
System	A piece of software, computer packages or manually managed asset that supports the administration of one or more areas within the academy	Capita SIMS, Parentpay, MyMaths

System Group	An umbrella term to describe the areas of school administration where systems that contain personal level data typically reside.	Curriculum Tools
Personal data	Information relating to a natural identifiable persons, whether directly or indirectly, name, address, online identifier	John Smith was born on 1.1.90. Jane Smith's Salary is £35,000
Special Category Data	These are highly sensitive pieces of information about individuals. They are important because under GDPR they are afforded extra protection in terms of the reasons you need to have access and process that information. In Education, it would also be best practice to treat subjects like FSM, SEN, CIN/CLA status as special category data	Tightly defined as data relating to racial or ethnic origin, political opinions, religious or philosophical beliefs, health, trade-union membership and health or sex life. Data relating to criminal offences is also afforded similar special protection
Educational record	The educational record is confined to information that comes from a teacher or other employee of a local authority or academy, the pupil or their parents. Communications about a particular child from head teachers and teachers at an academy and other employees at an education authority will therefore form part of that child's official educational record, as will correspondence from an educational psychologist engaged by the governing body under a contract of	
Information Commissioner	The independent person who has responsibility to ensure compliance with GDPR and can enforce measures against individuals or organisations who do not comply	
Lawful basis and conditions for processing	Specific Reasons set out in law, for which you can process personal data. There is one list for personal data (lawful basis article 6 and another list for processing special category data)	The processing is necessary for administering justice, or for exercising statutory or governmental functions. (Read the full list)

Automated decision making/Profiling	This is when machines/software apply rules to data and determine a fact about an individual based purely on specified rules. Typically it is the significance of the decision which drives the caution and concern.	
Subject Access Request	A person can request access to the information that is held about them and you have one calendar month to provide them with that information.	

27

GDPR POLICY APPENDICES

1. GDPR Management Structure and Framework
2. GDPR Steering Group Terms of Reference
3. Consent Form
4. Consent Letter to Parents
5. Privacy Notices to Parents and Carers
6. Privacy Notice for Staff
7. Template – Data Mapping/Data Asset Register
8. Template – Data Protection Impact Assessment
9. Template -Risk Management Process Flow Chart
10. Template – Reporting of a Data Breach Template
11. ICO Registration Certificate
12. List of Contact Details