The Societas Trust

Data Protection Policy

Date of Policy	2024
Reviewed and Agreed by	The Directors' Board
Last Review Date	9 July 2025
Next Review Date	Summer 2026

Contents

Part 1 Introduction and Key Definitions

1.1 Introduction

The Societas Trust and the Academies that form part of the Trust needs to gather and use certain information about individuals.

These individuals can include pupils, parents/carers, employees, suppliers, business contacts and other people the Trust or the Academy has a relationship with or may need to contact.

This policy describes how this personal data must be collected, handled and stored to meet the Trust/Academy data protection standards — and to comply with the law.

This data protection policy ensures that The Societas Trust and xxxxxx Primary Academy

- complies with data protection law and follows good practice
- protects the rights of pupils, staff, parents/carers and other stakeholders
- is open about how it stores and processes individuals' data
- protects itself from the risks of a data breach

This data protection policy is based on the six principles of the Data Protection Act (DPA) 2018 that personal data shall be:

1. processed lawfully, fairly and in a transparent manner
2. collected for specified, explicit and legitimate purposes
3. adequate, relevant and limited to what is necessary in relation to the purposes for which it is processed
4. accurate and kept up to date
5. kept in a form which permits identification of data subjects for no longer than is necessary
6. processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss or damage

1.2 Key Definitions

Data

The DPA describes how organisations, including The Societas Trust and xxxxxx Primary Academy must collect, handle and store personal information ('data').

Data is any information that the Trust/Academy collects and stores about individuals or organisations. Some data is more sensitive than others and particular care will be given to processing and managing this. Sensitive data includes:

- racial or ethnic origin;

- political opinions;
- religious or philosophical beliefs;
- trade union membership;
- data concerning health or sex life and sexual orientation;
- genetic data; and
- biometric data.

Data can be stored electronically, on paper or on other materials.

To comply with the law, personal information must be collected and used fairly, stored safely and not disclosed unlawfully.

Data Subject

A 'Data Subject' is someone whose details the Trust / Academy keeps on file. The data subject has the following rights under data protection legislation:

- to be informed
- to have access to data stored about them (or their children)
- to rectification if there is an error in the data stored
- to erasure if there is no longer a need for the school to keep their data
- to restrict processing (e.g. limit what their data is used for)
- to object to data being shared or collected

Although data protection legislation affords these rights to individuals, in some cases the obligations schools have to share data with the DfE etc override these rights (this is documented later in the policy under 'Privacy Notices').

Data Controller

The 'Data Controller' has overall responsibility for the personal data collected and processed and has a responsibility for ensuring compliance with the relevant legislation. They are able to delegate this to 'Data Processors' to act on their behalf.

The Trust/Academy is the 'Data Controller'.

Data Processor

A 'Data Processor' uses, collects, accesses or amends the data that the controller is authorised to collect or has already collected. It can be a member of staff or a third party company such as a curriculum software provider or a payroll provider.

Part 2 Organisational Arrangements

2.1 Overall Responsibility

The Societas Trust and xxxxxx Primary Academy will meet its obligations under the DPA by putting in place clear policies that focus on the key risks and in checking that control measures have been implemented and remain appropriate and effective.

2.2 Roles & Responsibilities

The Societas Trust is committed to ensuring that all its staff are aware of their 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 Data Protection Management Structure and Framework **(Appendix A**) within The Societas Trust will comprise representation as follows: A Data Protection Board Director, and within each Academy within the Trust there is a Data Protection Link Governor on the Local Governing Board who has individual academy responsibility together with the Headteacher who is the Data Protection Lead at each academy. The Members and Directors have delegated overall responsibility for Data Protection compliance to the CEO, Jon Lovatt, CEO and sub contracted the role of the DPO to SBM Services (UK) Ltd. The Trust Training and Compliance Manager acts as the main point of contact day to day between the DPO and each Academy. The Trust has set up an Emergency Management Committee in the event of Breaches and a Data Protection Steering Group who meet on a regular basis to deal with all Data Protection Issues. The Terms of Reference for the Steering Group can be found as **(Appendix B)**

The Local Governing Board for each Academy will:

- Establish and maintain a positive data protection culture.
- Ensure the Trust Data Protection policy has been implemented by the Academy and monitored for its effectiveness.
- Monitor and review data protection issues.
- Ensure that the academy provides adequate training, information, instruction, induction and supervision to enable everyone to comply with their data protection responsibilities.
- Review and act upon data protection compliance reports from the Data Protection Officer.
- Complete data protection and cyber security training annually as organised by the Academy.

The Headteacher / Data Protection Lead will

- Promote a positive data protection culture.
- Ensure the Data Protection Policy is approved by the Local Governing Board and reviewed annually.
- Ensure that all staff co-operate with the policy.
- Ensure all new staff are made aware of their responsibilities as part of their induction.

- Ensure that staff are competent to undertake the tasks required of them and have been provided with appropriate data protection training annually.
- Ensure all staff complete annual cyber security training to ensure they are aware of cyber risks
- Provide staff with equipment and resources to enable them to protect the data that they are processing.
- Ensure that those who have delegated responsibilities are competent, their responsibilities are clearly defined, and they have received appropriate training.
- Liaise with the Trust Compliance and Training Manager for advice on data protection related activities.

The Data Protection Officer will:

- Inform and advise the Trust/Academies of their obligations under data protection legislation.
- Monitor compliance with the legislation and report to the Trust Compliance and Training Manager on an ongoing basis.
- Co-operate with the supervisory authority (e.g. Information Commissioners Office) and act as the main contact point for any issues.
- Seek advice from other organisations or professionals, such as the Information Commissioners Office as and when necessary.
- Keep the Trust up to date with new developments in data protection issues for schools.
- Advise and guide the Trust/Academy on subject access requests and data breaches.

All Trust/Academy Staff will:

- Familiarise themselves and comply with the Data Protection Policy.
- Comply with the Trust/Academy data protection arrangements.
- Follow the data breach reporting process.
- Complete data protection and cyber security training annually as organised by the Trust/Academy.
- Ensure that any personal information they provide the Academy is accurate and up to date and inform the Academy of any changes, e.g change of address

Part 3 Detailed Arrangements & Procedures

3.1 Data Management

Data Registration

As Data Controller, The Societas Trust must register as a Data Controller on the Data Protection Register held by the Information Commissioner. The Societas Trust is registered and is due to renew on 17/10/25.

Data Protection Officer

As a public body, The Societas Trust is required to appoint a Data Protection Officer (DPO).

At The Societas Trust the DPO role is fulfilled by **SBM Services Limited**. Their contact details are Unit 12 Park Lane Business Centre, Park Lane, Langham, Colchester. CO4 5WR Tel 01206 671103 info@sbmservices.co.uk

The role of the DPO is to:

- Inform and advise the Trust/Academy and the employees about obligations to comply with all relevant data protection laws.
- Monitor compliance with the relevant data protection laws through annual audits.
- Be the first point of contact for supervisory authorities.

Data Protection Awareness

In order to ensure organisational compliance, all staff and other key stakeholders (e.g. governors, volunteers) will be made aware of their responsibilities under the data protection legislation as part of their induction programme, (both as a new employee/governor to the organisation or if an individual changes role within the school/academy).

Staff and governors/trustees will also be required to complete annual cyber security training to ensure that they are aware of cyber risks and understand the important role that they play in reducing the risk of a successful cyber attack.

Annual data protection refresher training will take place to reinforce the importance of staff and governors/trustees adhering to the legislation.

A record of the professional development undertaken by the individual will be retained on their training record.

Data Mapping

The Trust and each of the Academies has documented all of the data that it collects within a 'Data Flow Map'. This data inventory records:

- the data held
- what the data is used for
- how it is collected
- how consent is obtained
- how the data is stored
- what the retention period is
- who can access the data
- who is accountable for the data
- how the data is shared
- how the data is destroyed

For each data type, the probability of a data breach occurring is assessed (very high, high, medium, low or very low) and actions to be taken to mitigate the risk are recorded.

It is the responsibility of the Academy Business Manager to ensure the 'Data Flow Map' is kept up to date. The map should be a live document and updated regularly.

3.2 Third Party Suppliers Acting as Data Processors

As Data Controller, the Trust/Academy is responsible for ensuring that correct protocols and agreements are in place to ensure that personal data is processed by all subcontractors and other third parties in line with the principles of the data protection legislation.

Individuals within school who have a responsibility for securing contracts and agreements with such third parties are responsible for ensuring that all external data processing is contracted out in line with the principles of the DPA. These type of agreements include:-

- IT contracts and processes.
- Physical data and hard copy documents.
- Data destruction and hardware renewal and recycling financial and personnel information.
- Pupil and staff records.

Only third-party suppliers who can confirm they have appropriate technical, physical and organisational security to securely process data will be considered as suitable partners.

The procurement process will ensure that all contracts are suitable and reflect DPA requirements. Review of current and due consideration of future contracts will require this even if data processing is ancillary to the main purpose of the contract.

The external processor will confirm with the data controller that suitable security and operational measures are in place.

Any potential supplier or purchaser outside the EU will be obliged to confirm how they comply with the DPA and give contractual assurances.

A specific risk assessment may need to be undertaken if the data is sensitive, and if an increased risk is likely due to the nature, or proposed nature, of the processing.

A written agreement will be in place between the supplier and the Trust/Academy to confirm compliance with the DPA principles and obligations to assist the Trust/Academy in the event of a data breach or subject access request, or enquiries from the ICO.

The Trust/Academy must have the right conduct audits or have information about audits that have taken place in respect of the relevant processes of the supplier's security arrangements whilst the contract is in place, or whilst the supplier continues to have personal data that relates to the contract on its systems.

Any subcontracting must only be done with the written consent of the Trust/Academy as data controller. This must be the case for any further subcontracting down the chain. All subcontractors must confirm agreement to be bound by DPA principles when handling the Trust/Academy data, which shall also include cooperation and eventual secure destruction or return of data.

A 'Third Party Request for Information' form **(Appendix C)** should be completed for each request which summarises this information.

The Trust/Academy maintains evidence of the checks that have taken place for each of their third party suppliers.

The Academy Business Manager will inform the Trust Compliance & Training Manager if they receive a Third Party Request for Information.

3.3 Consent

As a Trust/Academy we will seek consent from staff, volunteers, young people, parents and carers to collect and process their data. We will be clear about our reasons for requesting the data and how we will use it. There are contractual, statutory and regulatory occasions when consent is not required. However, in most cases, data will only be processed if explicit consent has been obtained.

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

We may seek consent from young people also, and this will be dependent on the child and the reason for processing.

Privacy Notices

In order to comply with the fair processing requirements of the DPA, the Trust/Academy will inform their staff, parents/carers of all pupils and governors/trustees of the data they collect, process and hold on them, the purposes for which the data is held and the third parties (e.g. LA, DfE, etc) to whom their data may be passed, through the use of 'Privacy Notices'.

Privacy notices are available to staff, parents and governors/trustees through the following means:

- Trust / Academy website
- Policy folders
- Staff Handbook

Privacy notices will be reviewed on an annual basis.

The Use of Images (Pupil & Staff)

Occasionally the Trust/Academy may take photographs of its pupils or staff members. These images could be used as part of internal displays, printed publications, the website or our social media accounts.

The Academy will seek consent from all parents to allow the photography of pupils and the subsequent reproduction of these images (see **Appendix D** – Pupil/Parental Consent Form)

The Academy will seek consent from all members of staff to allow their photography and the subsequent reproduction of these images. (Please refer to the Staff Photo Consent form within the Photography and Images Policy)

Consent will last for the length of time the child is a pupil at the academy and beyond.

Parents and staff are given the opportunity to opt in. It is not permissible to assume they are opting in.

Generic consent for all uses of images is not acceptable; parents and staff must give consent to each medium.

Parents and staff must be given the opportunity to withdraw their consent at any time. This should be given in writing to the school/academy, however a verbal withdrawal of consent is also valid and should be reported to the headteacher immediately.

Consent should be recorded on the school MIS and the school whole school consent form

If images of individual pupils are published, then the name of that child should not be used in the accompanying text or caption unless specific consent has been obtained from the parent prior to publication.

The Academy 'Parental Consent' and 'Staff Consent' forms are used to seek consent when they join the organisation.

Accurate Data

The Trust/Academy will endeavour to ensure that the data it stores is accurate and up to date.

When a pupil or member of staff joins the Trust/Academy they will be asked to complete a form providing their personal contact information (e.g. name, address, phone number, NI number for staff), next of kin details, emergency contact and other essential information. At this point, the Trust/Academy will also seek consent to use the information provided for other internal purposes (such as promoting school events, photography).

The Trust/Academy will undertake an annual data collection exercise, where current staff and parents will be asked to check the data that is held about them is correct. This exercise will also provide individuals with the opportunity to review the consent they have given for the Trust/Academy to use the information held for internal purposes.

Parents/carers and staff are requested to inform the Trust/Academy when their personal information changes.

Withdrawal of Consent

Consent can be withdrawn, subject to contractual, statutory or regulatory constraints. Where more than one person has the ability to provide or withdraw consent, the Trust/Academy will consider each situation on its merits and within the principles of the DPA, child welfare, protection and safeguarding principles.

Parents/carers and staff are requested to inform the school in writing if they wish to withdraw consent.

3.4 Associated Data Protection Policies/Processes

- CCTV
- Complaints
- Code of Conduct
- Data Breaches
- Data Privacy Impact Assessments
- ICT Usage Agreements
- Data Retention
- Subject Access Requests
- Third Party Requests for Information
- Use of Personal Devices

CCTV

The Trust/Academy uses closed circuit television (CCTV) images to reduce crime and monitor the buildings in order to provide a safe and secure environment for pupils, staff and visitors, and to prevent loss or damage to the school property. The Trust/Academy has a CCTV Policy in place which documents:

- why CCTV is used
- where cameras are sited
- whether covert monitoring is undertaken
- how long images are retained for
- who has access to the images
- what the complaints procedure is

Complaints

Complaints will be dealt with in accordance with the Trust/Academy Complaints Policy or escalate to our Data Protection Office. An individual may contact the Information Commissioner's Office (ICO) if they are not satisfied with how a complaint has been dealt with by the Trust/Academy. The telephone number for the ICO is 0303 123 1113.

Code of Conduct & Confidentiality

The Staff/Governor/Volunteer policies sets out the expectations the Trust/Academy has in relation to maintaining confidentiality. All staff, governors/trustees and volunteers are required to sign on an annual basis.

Data Breaches

Although the Trust/Academy takes measures against unauthorised or unlawful processing and against accidental loss, destruction or damage to personal data as set out in this policy and the supporting policies referred to, a data security breach could still happen. Examples of data breaches include:

- Loss or theft of data or equipment on which data is stored (e.g. losing an unencrypted USB stick, losing an unencrypted mobile phone).
- Inappropriate access controls allowing unauthorised use.
- Equipment failure.
- Human error (e.g. sending an email to the wrong recipient, information posted to the wrong address, dropping/leaving documents containing personal data in a public space).
- Unforeseen circumstances such as fire or flood.
- Hacking attack.
- 'Blagging' offences where information is obtained by deceiving the Trust/Academy.

However the breach has occurred, the following steps should be taken immediately:

1. **Internal Notification:** Individual who has identified the breach has occurred must notify the Academy Business Manager / Headteacher. The Academy Business Manager must then notify the Trust Compliance and Training Manger by forwarding the completed Data Breach Incident form **(Appendix E**). The Trust Compliance & Training Manager who will also notify the DPO for their records and they will add their advice & comments to the Incident Form. A record of the breach should be created using the following templates:
    a. Data Breach Incident Form **(Appendix E)**
    b. Data Breach Log (Trust Template saved in dropbox)
    c. Evidence Log **(Appendix F)**

2. **Containment:** Academy Business Manager/Headteacher in liaison with the Trust Compliance and Training Manager & DPO to identify any steps that can be taken to contain the data breach (e.g. isolating or closing the compromised section of network, finding a lost piece of equipment, changing access codes) and liaise with the appropriate parties to action these.

3. **Recovery:** Academy Business Manager/Headteacher in liaison with the Trust Compliance and Training Manager & DPO to establish whether any steps can be taken to recover any losses and limit the damage the breach could cause (e.g. physical recovery of equipment, back up tapes to restore lost or damaged data)

4. **Assess the risks:** Before deciding on the next course of action, the Academy Business Manager/Headteacher in liaison with the Trust Compliance and Training Manager & DPO to assess the risks associated with the data breach giving consideration to the following, which should be recorded in the Part B of the Data Breach Incident form:

    a. What type of data is involved
    b. How sensitive is it?
    c. If data has been lost/stolen, are there any protections in place such as encryption?
    d. What has happened to the data?
    e. What could the data tell a third party about the individual?
    f. How many individuals data have been affected by the breach?

g. Whose data has been breached?
h. What harm can come to those individuals?
i. Are there wider consequences to consider such as reputational loss?

5. **Notification to the Information Commissioners Office (ICO):** Following the risk assessment in step 4, the DPO should notify the ICO within 72 hours of the identification of a data breach if it is deemed that the breach is likely to have a significant detrimental effect on individuals. This might include if the breach could result in discrimination, damage to reputation, financial loss, loss of confidentiality or any significant economic or social disadvantage.

   The DPO should contact ICO using their security breach helpline on 0303 123 1113, option 3 (open Monday to Friday 9am-5pm) or the ICO Data Breach Notification form can be completed and emailed to casework@ico.org.uk.

6. **Notification to the Individual:** The Trust/Academy and DPO must assess whether it is appropriate to notify the individual(s) whose data has been breached. If it is determined that the breach is likely to result in a high risk to the rights and freedoms of the individual(s) then they must be notified by the Trust/Academy

7. **Evaluation:** The Trust/ Academy and DPO should assess whether any changes need to be made to the Trust/Academy processes and procedures to ensure that a similar breach does not occur.

Data Privacy Impact Assessments

When considering the purchase of a new service or product that involves processing personal data, a Data Privacy Impact Assessment must be completed by the Academy Business Manager. If risks are identified as part of the assessment then appropriate steps to mitigate this risk must be implemented. If these risks are deemed to be 'high risk' then the DPO should consult with the ICO prior to implementation.

The 'Data Privacy Impact Assessment' form must be used for each new service/product. **(Appendix G)**

ICT Acceptable Use Agreements

The Trust/Academy has an ICT Acceptable Use Agreements in place which staff, governors/trustees and volunteers are required to sign on an annual basis. This agreement sets out the expectations the Trust/Academy has in relation to staff safely and securely using the IT network.

Information sharing in an employee medical or mental health emergency

Data protection law allows the Trust/Academy to share personal information in an urgent or emergency situation, including to help prevent loss of life or serious physical, emotional or mental harm.

During a medical or mental health emergency where there is risk of serious harm to staff or to others the Trust/Academy will share necessary and proportionate information without delay with relevant and appropriate emergency services or health professionals. The Trust/Academy may also share necessary and proportionate information with the member of staff's next of kin or emergency contact.

The Trust/Academy will use their judgement in each specific situation, sharing only what is necessary and proportionate to the circumstances. The Trust/Academy may decide that, whilst it may be necessary and proportionate to provide the emergency services with a full account of the situation, it is only appropriate to provide the member of staff's emergency contact with more limited details.

The Trust/Academy staff privacy notice covers this sharing of data.

Data Retention

The Trust/Academy recognises that by efficiently managing its records, it will be able to comply with its legal and regulatory obligations which will also contribute to the effective overall management of the school.

The Trust/Academy has a Data Retention Policy in place which sets out how it will:

- safely and securely store data (both digital and hard copy data)
- retain data
- dispose of data

The retention schedule is based on the good practice advice provided by the Institute of Records Management Society (IRMS) for schools.

Subject Access Requests

Any individual, person with parental responsibility or young person with sufficient capacity has the right to ask what data the Trust/Academy holds about them and can make a Subject Access Request (SAR).

A SAR can be made verbally or in writing. A 'Subject Access Request' form (**Appendix H)** is included within this policy to support individuals with making their request. To avoid any delays during school closure periods requests should be made electronically during school closure periods.

The Academy Business Manager has been designated as the individual who will coordinate the response to a SAR and will acknowledge the request.

The Trust/Academy is required to provide the individual with the data it holds on them within one calendar month. The Trust/Academy can extend the time to respond by a further two months if the request is complex or they have received a number of requests from the individual. The individual must be contacted at the earliest opportunity, but at least within one month of the Trust/Academy receiving their request, and explain why the extension is necessary.

The response to the SAR will generally be provided in the same format that the request was submitted by the individual.

It is permissible to ask the individual who has made the request to be more specific about the information that they require in order to ensure that the information they are provided with meets their requirements rather than providing lots of information that may not be relevant to their query.

Evidence of the identity of the person making the request and their relationship to the pupil may be required prior to any disclosure of information. This should be recorded on the SAR Log.

All SARs should be recorded on the SAR log and the Academy Business Manager should inform the Trust Training and Compliance Manager. The DPO (SBM Services UK Ltd) will be informed so they can provide guidance where applicable.

Exemptions to a SAR may include:

- Third party data, for example information about other pupils or adults that are not the data subject or individual making the request
- Data that could lead to a risk of harm to the data subject or individual making the request
- Information that is not the personal data of the data subject or individual making the request
- Management information
- Records relating to a live investigation (e.g. an ongoing complaint, behaviour, grievance, disciplinary matter etc)
- Education, Health, Social Work records
- Examination marks and scripts
- Safeguarding records
- Special educational needs records
- Parental records and reports
- Legal advice and proceedings
- Adoption and Court records and/or reports
- Regulatory activity and official requests e.g. DfE statistical information
- National security, Crime and taxation
- Journalism, literature and art
- Research history, and statistics
- Confidential references

For full details of exemptions to SARs please visit the ICO website: A guide to the data protection exemptions | ICO

A copy of the information will be supplied to the individual free of charge; however, the school may impose a 'reasonable fee' to cover the administrative costs of complying with requests that are manifestly unfounded or excessive or if an individual requests further copies of the same information. Where a request is manifestly unfounded, excessive or repetitive, a reasonable fee will be charged. All fees will be based on the administrative cost of providing the information.

When responding to a Subject Access Request the following supplementary information should be provided with the response: see SAR response template **(Appendix I)**

- The purpose of the data processing
- Source of the data
- Who the data was shared with
- Retention period
- Whether any automated decision making was undertaken

Third Party Requests for Information

Occasionally the Trust/Academy may receive a request for information on a pupil or member of staff by a third party, such as the police or social services. This would be separate to statutory requests that come through from the DfE or LA, for example, which are covered within the privacy notices.

The police do occasionally ask for personal data as part of an inquiry, but they don't have the automatic right to receive information about our staff or pupils. You should not feel pressured into handing over personal information. There is a special process the police are required to follow to access personal data for certain crime-related purposes.

However, child protection and safeguarding can take priority over data protection. The Children Act 1989 and 2004, Education Act 1996 and 2002 all emphasise the importance of sharing information responsibly where safeguarding is an issue.

Every situation should be assessed on its individual circumstances, and a distinction must be made at this time whether the information has been requested on an emergency basis, (where there is immediate and significant risk to the life and/or limb of a person), or whether the information is required as part of a routine investigation (where there is no immediate threat of harm).

If there is any doubt, then the school's legal advisor should be contacted for advice.

Any decisions about disclosure on safeguarding requirements should be recorded. The member of staff who has disclosed the data should make a record in the pupil or staff file of the following:

- Information that has been disclosed
- Who it has been disclosed to (person, position and agency)
- Who within the school authorised the release of the data
- Date & time of the decision

A 'Third Party Request for Information' form **(Appendix C)** should be completed for each request which summarises this information.

The Academy Business Manager must inform the Trust Compliance and Training Manager and the DPO will be advised.

Use of Personal Devices

The Trust/Academy recognises the benefits of mobile technology and is committed to supporting staff in the acceptable use of mobile devices. The Trust/Academy follows the 'ICT and Electronic Devices' Policy which sets out how non-school owned electronic devices, e.g. laptops, smart phones and tablets, may be used by staff members and visitors to the school.