Data protection policy

Approved by:	Board of Trustees	Date: May 2018
Last reviewed on:	19 October 2023	
Next review due by:	31 October 2024	

1. Introduction

1.1 The Gosforth Federated Academies Ltd is committed to ensuring that all data collected about staff, pupils, parents and visitors is collected, stored and processed in accordance with its legal and regulatory obligations.

1.2 This policy sets out the expected behaviours of employees in relation to the collection, use, retention, transfer, disclosure and destruction of personal data belonging to data subjects.

1.3 The Trust's leadership is fully committed to ensuring continued and effective implementation of this policy and expects all staff to share in this commitment. Any breach of this policy will be taken seriously.

1.4 The policy is based on guidance published by the Information Commissioner's Office and model privacy notices published by the Department for Education. It also takes into account the requirements of the UK General Data Protection Regulation (UK GDPR) and the provisions of the Data Protection Act 2018. The policy also complies with the Master Funding Agreement, its associated Supplemental Funding Agreements and the Trust's Articles of Association.

2. Scope

2.1 This policy applies to all individuals where a data subject's personal data is processed.

2.2 The Trust processes personal information to enable us to provide education, training, welfare and educational support services, to administer school property, and to support and manage our employees.

2.3 The policy applies to all processing of personal data in electronic form, including email and documents created with word processing software, or where it is held in manual files that allows ready access to information about individuals.

2.4 We also use CCTV to assure health and safety requirements, safeguarding and welfare, and the prevention and detection of crime. The policy reflects the ICO's code of practice for use of surveillance cameras and personal information.

3. Accountability and governance

3.1 This policy applies to all staff employed by the Trust, and to external organisations or individuals working on the Trust's behalf. Staff who do not comply with this policy may face disciplinary action.

3.2 The Board of Trustees has overall responsibility for ensuring that the Trust complies with all relevant data protection obligations.

3.3 The Gosforth Federated Academies Ltd processes personal information relating to pupils, staff, parents and visitors and, therefore, is defined as a Data Controller. The

Trust is registered as a Data Controller with the Information Commissioner's Office and renews its registration annually.

3.4 Article 5(2) of the GDPR also requires that "the controller shall be responsible for, and be able to demonstrate, compliance with the principles." The academy Principals act as the representative of the data controller on a day-to-day basis.

3.5 The Trust has appointed a Data Protection Officer who is responsible for overseeing the implementation of this policy, monitoring compliance with data protection law, and developing related policies and guidelines where applicable.

3.6 The DPO will provide an annual report of their activities directly to the Board of Trustees and, where relevant, report to the board their advice and recommendations on data protection issues.

3.7 The DPO can be contacted at schoolsdpo@veritau.co.uk, or by writing to:

Veritau
West Offices
Station Rise
York
YO1 6GA

3.8 In addition, the Trust has designated data protection advisors and contacts in each school to ensure data protection principles and requirements are observed and to promote a strong culture of data protection across the Trust.

3.9 To confirm that an adequate level of compliance is being achieved the Trust works with the DPO to ensure that an annual data protection compliance audit is carried out to:

- review data protection responsibilities;
- continue to raise awareness;
- ensure appropriate training of staff;
- assure the effectiveness of operational practices;
- confirm the currency of policies and privacy notices; and to
- verify that procedures are in place to redress poor compliance.

3.10 When designing and implementing new, or changes to existing systems or processes a Data Protection Impact Assessment (DPIA) will be conducted and approved by the Data Protection Officer to ensure that all data protection requirements are identified and addressed.

4. The Data Protection Principles

4.1 Under the UK GDPR, the data protection principles set out the main responsibilities for organisations. Article 5 of the UK GDPR requires that personal data shall be:

a) processed lawfully, fairly and in a transparent manner in relation to individuals;

b) collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall not be considered to be incompatible with the initial purposes;

c) adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed;

d) accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay;

e) kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes subject to implementation of the appropriate technical and organisational measures required by the UK GDPR in order to safeguard the rights and freedoms of individuals; and

f) processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.

5. Lawful basis for processing

5.1 In accordance with the UK GDPR the Trust must have a valid lawful basis in order to process personal data and special category data.

5.2 The lawful bases for processing are set out in Article 6 of the UK GDPR. At least one of these must apply whenever the Trust processes personal data:

(a) Consent: the individual has given clear consent for the Trust to process their personal data for a specific purpose.

(b) Contract: the processing is necessary for a contract the Trust has with the individual, or because they have asked the Trust to take specific steps before entering into a contract.

(c) Legal obligation: the processing is necessary for the Trust to comply with the law (not including contractual obligations).

(d) Vital interests: the processing is necessary to protect someone's life.

(e) Public task: the processing is necessary for the Trust to perform a task in the public interest or for its official functions, and the task or function has a clear basis in law.

(f) Legitimate interests: the processing is necessary for the Trust's legitimate interests or the legitimate interests of a third party unless there is a good reason to protect the individual's personal data which overrides those legitimate interests. (This cannot apply to public authorities processing data to perform its official tasks.)

5.3 As a public authority the Trust has considered the 'public task' basis as the most appropriate reason for the majority of its processing. In some circumstances the Trust has agreed that 'consent', 'legal obligation' and 'legitimate interest' are more appropriate bases for processing data. The Trust's lawful bases for processing personal data are documented in the Trust's Information Audit (February 2018).

5.4 The Trust has informed people about the lawful basis for processing their personal data and these are included in its privacy notices.

6. The rights of data subjects

6.1 The UK GDPR and the DPA 2018 provides the following rights for individuals:

- The right to be informed
- The right of access
- The right of rectification
- The right to erase
- The right to restrict processing
- The right to data portability
- The right to object
- Rights in relation to automated decision making and profiling

6.2 The Gosforth Federated Academies Ltd ensures that procedures are in place to enable the efficient processing of data subjects' rights:

- Fair processing information is provided through the Privacy Notices published on the Trust's website;
- Retrieval and verification of personal data and supplementary information is permitted through the Subject Access Request (SAR) process (see Appendix A);
- Should personal data or information be found to be inaccurate or incomplete the Trust will resolve this as appropriate, where a SAR request for rectification is submitted to the Data Protection Officer;
- The Trust will not apply the right to erase where personal data is processed lawfully to comply with a legal obligation for the performance of a public task or exercise of its official authority;

- The processing of personal data will be restricted through the submission of a SAR where the accuracy of data is contested; where an individual objects to the processing; when processing is deemed as unlawful; or where information is no longer needed but the personal data is required by an individual to establish, exercise or defend a legal claim;
- When responding to a SAR the Trust will provide personal data to a subject in a structured, commonly used and machine-readable form (subject to technical compatibility), and it will be provided free of charge;
- Where an objection to data processing is raised, the rust will stop processing the personal data unless there are compelling legitimate grounds for the processing that override the data subject's right. Individuals will be informed of their right to object at the point of first communication. This is published in the Trust's Privacy Notices;
- No automated individual decision-making and profiling is undertaken by the Trust.

7. Data security

7.1 The UK GDPR requires personal data to be processed in a manner that ensures its security. This includes protection against unauthorised or unlawful processing and against accidental loss, destruction or damage. It requires that appropriate technical or organisational measures are used.

7.2 The Gosforth Federated Academies Ltd fully recognises its responsibilities to protect personal information that staff collect and use, including requirements to prevent personal data being accidentally or deliberately compromised. The Trust adopts physical, technical and organisational measures to ensure the security of personal data.

7.3 General staff guidelines

7.3.1 The only people able to access data covered by this policy are those who need it for their work.

7.3.2 Data should not be shared informally. When access to confidential information is required, staff should request it from appropriate managers.

7.3.3 The Trust will provide training to all staff and those responsible for academy governance to help them understand their responsibilities when handling data.

7.3.4 Employees should keep all data secure, by taking sensible precautions and following the guidelines below.

7.3.5 In particular, strong passwords must be used, and they should never be shared.

7.3.6 Personal data should not be disclosed to unauthorised people, either within the Trust or externally.

7.3.7 Data should be regularly reviewed and updated if it is found to be out of date. If no longer required is should be deleted and disposed of appropriately.

7.3.8 Staff should seek guidance from managers or the Data Protection Officer if they are unsure about any aspect of data protection.

7.4 Data storage

7.4.1 When data is stored on paper it should be kept in a secure place where unauthorised people cannot see it.

7.4.2 These guidelines apply to data that is usually stored electronically but has been printed out for operational purposes:

- When not required the paper or files should be kept in a locked drawer or filing cabinet;
- Staff should make sure paper, and printouts are not left where unauthorised people could see them, like on a printer or copier;
- Data printouts should be shredded and disposed of securely when no longer required

7.4.3 When data is stored electronically it must be protected from unauthorised assess, accidental deletion and malicious hacking attempts:

- Data should be protected by strong passwords that are changed regularly and never shared between employees;
- If data is stored on removable media these should be kept locked away securely when not being used;
- Data should only be stored on designated drives and servers, and should only be uploaded to approved computing services;
- Servers containing personal data should be sited in a secure location away from general office space;
- Data should be backed up frequently. Those backups should be tested regularly in line with the IT managed service backup procedures;
- Data should never be saved directly to laptops or other mobile devices like tablets or smart phones;
- All servers and computers containing data should be protected by approved security software and a firewall

7.4.4 The IT managed service will ensure that all systems, services, software and equipment meet acceptable security standards.

7.5 Data use

7.4.5 Personal data is at greatest risk of loss, corruption or theft when it is accessed and used. When working with personal data staff should ensure that:

- The screens of computers are always locked when unattended;
- Data must be encrypted if being transferred or stored electronically;

- Data should not be saved to staff's own computers, devices, or personal email addresses.

7.6 Data accuracy

7.6.1 The law requires the Trust to take reasonable steps to ensure that data is kept accurate and up to date. It is the responsibility of all staff who work with data to take practical measures to ensure it is kept as accurate and up to date as possible.

7.6.2 Data will be held in definitive staff or pupil personal files. Staff should not create any unnecessary additional data sets, or files relating to pupils and staff.

7.7 Data breaches

7.7.1 The UK GDPR introduced a duty on all organisations to report certain types of personal data breach to the relevant supervisory authority. In the UK the supervisory authority is the Information Commissioner's Office (ICO).

7.7.2 The Trust must inform the ICO of any breach within 72 hours of becoming aware of that breach, where feasible.

7.7.3 All members of staff have an obligation to report actual or potential data protection compliance failures to the Data Protection Officer without delay.

7.7.4 The Data Protection Officer will investigate the reported breach in order to determine whether or not the ICO and affected individuals need to be notified.

7.7.5 A register of personal data breaches will be maintained, regardless of whether these have been notified or not.

7.7.6 A separate policy and procedure has been developed to deal with the reporting of a data breach. Please refer to the Trust's website for further information or contact the DPO at schoolsdpo@veritau.co.uk

8. International transfers

8.1 The UK GDPR imposes restrictions on the transfer of personal data outside of the European Economic Area (EEA). These restrictions are in place to ensure that the level of protection of individuals afforded by the UK GDPR is not undermined.

8.2 If the Trust is requested to transfer a pupil file outside the EEA because a pupil has moved into that area, please refer the request to the Data Protection Officer.

9. Data retention

9.1 In accordance with UK GDPR principles and to ensure fair processing the Trust will not retain personal data for longer than necessary in relation to the purpose for which it was originally collected, or for which it was further processed.

9.2 The timeframes for retaining personal data are set out in the Trust's Records Retention and Management Policy. This takes into account the legal and contractual requirements that influence retention periods.

9.3 All personal data will be deleted or destroyed as soon as possible where it has been confirmed that there is no longer a need for it to be retained.

10. Subject Access Request (SAR)

10.1 Individuals have the right to access their personal data and supplementary information. The right of access allows individuals to be aware of and verify the lawfulness of the Academy's processing.

10.2 In accordance with data subjects' rights the Trust will provide a copy of requested information free of charge. However, a reasonable fee will be applied if the request is found to be manifestly unfounded, excessive, or repetitive.

10.3 SARs will be responded to within at least one month of receipt. A further two months may be applied where the request is considered complex or numerous and this will be communicated to individuals at the time of the request.

Gosforth Group

SUBJECT ACCESS REQUEST (SAR)

Please complete this form if you wish to exercise your rights in relation to:

- Getting access to your personal information;
- Raising an objection or restricting your data processing;
- Rectifying or erasing information that you think is incorrect or unlawful;

When you have completed the form please print, sign and send to the Data Protection Officer, c/o Veritau, West Offices, Station Rise, York, YO1 6GA or email schoolsdpo@veritau.co.uk

In order for the Trust to release or amend any personal data, and to protect your confidentiality you will need to supply proof of identity. Acceptable evidence is an official identity document containing a photograph, such as a current driving license or passport. Please bring your ID to the appropriate school reception for verification when advised to do so.

Details of the person making the request:

Title:	
First name(s):	
Last name:	
Date of birth:	
Address:	
Telephone:	
Email:	

If you are making this request on behalf of another person you must enclose with the request a signed authority from them to do so. If you are making the application because the data subject lacks capacity to make the application in their own right, please outline your authority to make the application in their stead, enclosing evidence that you have that authority.

Details of the Data Subject:

Title:	
First name(s):	
Last name:	
Date of birth:	
Address:	
Telephone:	
Email:	
Relationship to Data Subject:	

Describe the information you are requesting, or whether you wish to raise an objection, restriction, erasure, or rectification.

Please be as specific as possible and include all relevant detail about your request and about what exact information you wish to access or verify. Please note if insufficient detail is provided, we may have to come back to you to seek clarification.

Declaration: I certify the information on this form is true and correct

Signed:	
Date:	

If as a result of your request, you are dissatisfied with the way the Trust is using your personal data you should raise this matter with the Data Protection Officer at the address provided above. We will do everything we can to put matters right and if we disagree with you, we will tell you our reasons.