Data Protection Policy

1. Introduction

1.1. Background

Our Trust and Academies ("we") collect personal data about the people we deal with during the course of carrying out our business and delivering our services. Such people include our pupils, their parents or guardians ("guardians"), employees (at Central Services as well as teachers and support staff at our Academies), our suppliers and other business contacts.

This policy document sets out the approach we take towards managing this personal data to ensure we meet the data protection requirements set out in the General Data Protection Regulation ("GDPR"), any UK specific implementation of aspects of the Regulation into UK law and any guidance the Information Commissioner's Office, the Department for Education or European Data Protection Board provide.

We take data protection seriously and place a high importance on the correct and lawful processing of all personal data as well as respecting the rights and privacy of our pupils, their guardians and our employees. As such, this policy sets out the Trust and Academy procedures that are to be followed, by all employees when dealing with personal data across our organisation.

1.2. Data protection

In May 2018, the GDPR came into force across the whole of Europe, including the UK. The UK government also implemented a new Data Protection Act 2018. Together these laws constitute the data protection regime for the UK.

1.2.1. Key definitions

- "Personal data" relates to any information about an identifiable natural person (the "Data Subject") either directly or indirectly

- "Processing" means any activity carried out on the personal data including storage, collection, organisation, manipulation, destruction and general use

- A "Data Subject" is the person whose data it is that is being collected or processed by the Data Controller and/or the Data Processor, e.g. our pupils, their guardians, employees, etc.

- "Data Controller" is an organisation who determines the purposes of processing of data – typically this is the organisation that has collected the data in the first place and wishes to process it. So, for our pupils', guardians' and employees' data we are a Data Controller

- "Data Processor" is an organisation who processes data on behalf of the Data Controller (typically a third party)

1.2.2. Data protection principles

Controls around the use of data are governed by a set of principles, which state that data must be:

- Processed lawfully, fairly and transparently
- Collected only for specified or legitimate purposes and not further processed outside the original purpose for collection
- Relevant and necessary for the purposes for which they have been collected (i.e. we should not collect any data that we don't need)
- Accurate and kept up to date
- Only kept for as long as the data is required. Where data is no longer required it must be deleted or anonymised
- Kept and processed securely

It is up to the Data Controller or Processor to be able to demonstrate compliance with these principles (this is the principle of "accountability").

1.2.3. Lawfulness of processing

For processing to be lawful, data can only be processed when one of the following conditions applies:

- Where the Data Subject has given consent
- Where processing is required for the performance of a contract (e.g. we can process pupil data for the purposes of using that data whilst they are a pupil at an Academy)
- Where processing is required to comply with a legal obligation (e.g. as required by safe guarding laws or by the DfE)
- Where processing is necessary to protect the vital interests of the Data Subject
- Where processing is carried out in the public interest
- Where processing is carried out in the legitimate interests of the Data Controller, but without detriment to the Data Subject

1.2.4. Data subject rights

Under the GDPR, Data Subjects have the following rights:

- The right to be informed (including when the data was not obtained directly from them) about who has their data, what it's used for, who will have access to the data and their rights to object, withdraw consent, etc.

- The right to request whether data is being processed by the Data Controller and if so what data and how (this is a subject access request)
- The right to have their data updated and kept up to date
- The right to erasure ("right to be forgotten") of their data when the data is no longer needed, when consent has been withdrawn or if it has been unlawfully processed
- To restrict, in certain circumstances, the processing of their data
- The right to data portability allowing a Data Subject to request copies of their data in a format compatible with another system for their own use or to import into a third-party system
- The right to object to the processing under legitimate interests, for direct marketing purposes, for profiling or research
- The right to object to automated decision making

1.3. What data is covered by data protection?

Personal data is defined as any information which identifies a living individual. Generally, this will include data such as name, address, email addresses, telephone numbers but specifically for us it would also include:

- Other information about a pupil such as health, behavioural information, exam results, attendance information, special education needs, etc. and details of their guardians and past school records
- Payroll and other employment records (sick notes, health information, performance data, etc.) for employees
- Third-party suppliers of services to the Trust and Academies

2. Scope

This policy document applies to <u>all</u> employees, including full-time, part-time, contractors and temporary staff at Central Services and at our Academies.

3. Roles and responsibilities

3.1. All employees have a responsibility to ensure data protection compliance, however, these people have key areas of responsibility:

<u>The Trust Senior Management Team, Board of Trustees and Academy Councillors</u>

The Board of Trustees is ultimately responsible for ensuring adequate data protection controls are in place across the Trust and within Academies.

Academy Principals

Academy Principals have a duty to ensure their Academy applies the principles of data protection within the Academy, as set out by the Trust's policies and guidance.

Data Protection Officer

The Data Protection Officer is responsible for:

- Informing and advising the Trust and Academies on data protection compliance, including keeping the Board of Trustees updated about data protection responsibilities, risks and issues across the Trust
- Monitoring overall data protection compliance across the Trust including reviewing (annually) all data protection resources made available to the Trust, including this policy, other policies, guidance and support information
- Providing data protection guidance on new projects where data is involved across the Trust, including carrying out data protection impact assessments
- Ensuring adequate training is in place for all employees
- Dealing with data protection and privacy related questions from any part of the Trust or Academies
- Act as the contact point for the ICO on any issues relating to data protection compliance across the Trust and Academies
- Act as a contact point for pupils, guardians, employees and other Data Subjects
- Dealing with or advising on, Data Subjects' rights, including dealing with or advising on subject access requests, rights to erasure and portability
- Advising on any requests to access data (pupils, guardians or employees) from external third parties, for example law enforcement and government offices
- Carrying out due diligence and ensuring appropriate data processing agreements are in place for any third parties we use to share or store personal data

The Trust's Data Protection Officer is:

Mark Gracey
Mark.gracey@woodard.co.uk
07833 297193

Data Protection Champions

Each Academy will appoint a Data Protection Champion who is responsible for:

- Being a contact point on-site at the Academy relating to data protection matters
- Working with the Trust Data Protection Officer to ensure data protection compliance across the Academy
- Assisting the Trust Data Protection Officer when required, with data protection compliance matters within the Academy

IT Managers

IT Managers across the Trust and Academies are responsible for:

- Ensuring all IT systems and use of technology is compliant and in line with this policy
- Maintaining IT security across the business and ensuring the security of systems is kept up to date
- Assisting the Data Protection Officer and Champions with assessing the security aspects of any third-party systems that may be used to handle the company's data

HR Managers

HR Managers are responsible for ensuring that employee data is processed in line with this policy and any other rules or guidance relating to the use of employee data across the Trust

3.2. All employees will familiarise themselves with this policy and any associated policies, relating to the processing of personal data and ensure their processing of personal data is within the rules set out within these policy documents. Specifically, all employees should ensure:

- All personal data accessed, used or processed during their duties is kept and processed securely and in line with our IT security policies
- No personal data should be disclosed verbally, in writing or by any other means to any third party, without consent from the company's Data Protection Officer
- No company systems should be accessed for any reason other than for the purposes of carrying out their duties as an employee
- They contact the Data Protection Officer or their local Data Protection Champion if they are aware of an issue or are uncertain about any aspect of processing data or data protection

3.3. Any breach of this policy or any associated policy may result in disciplinary action in line with the employment contracts

4. Collection of personal data

4.1. Whenever we collect data, we will only ask for data that is needed for the circumstances for which we're collecting it. For example, when taking on a new pupil we will only collect the necessary information in order to support the education of the pupil

4.2. Where we need consent for the purposes of processing we will:

- Be open and transparent about why we are collecting the data and what is being consented to
- Provide an option for the Data Subject to provide their consent
- We will not provide any pre-ticked options or use any wording that could be missed or misconstrued by the Data Subject to "trick" them into consenting
- We will record the place, time and situation by which that consent was given and maintain a record of consents given

4.3. In all circumstances, when collecting data, we will provide the following information (in our privacy statements or promises):

- Details of who we are, why we're collecting the data, what it will be used for and how long we will use and keep the data, and the legal basis for processing
- Details of our Data Protection Officer and how they can be contacted
- Details of the Data Subject's rights:
    - Data Subject access requests
    - Have their data corrected if details change
    - Have their data deleted when it is no longer needed
    - Object to processing
    - Right to complain to the Information Commissioner's Office
- Details of how to withdraw consent (when consent is the lawful basis of processing)

4.4. Where we make use of data supplied by a third party, in addition to the items listed in 4.3, we will also provide details of where the data came from. The information will be given to the Data Subject at the first opportunity (but not more than one calendar month from receiving the data).

5. Use of personal data

5.1. We will only process personal data supplied to us for its original purpose. We will not reuse the data for any other purpose unless it is lawful for us to do so (e.g. we have consent from the Data Subject).

5.2. Where "legitimate interest" is the lawful basis for processing it will be possible to demonstrate that such processing is not harmful to the Data Subject's rights and the reason for processing as a legitimate interest documented

5.3. Where we process personal data for marketing purposes, we will make sure that we abide by all rules relating to the use of data for marketing purposes, such as the Privacy and Electronic Communications Regulations 2003 and make sure we have processes in place to ensure that we can manage any opt-outs of the marketing. If you are unsure whether you have the right permissions for marketing, the Data Protection Officer or your local Data Protection Champion should be consulted

5.4. Where we take and use photographs of pupils or employees we will do so in accordance with our photograph policy or guidance

6. Storing data

6.1. All personal data, particularly data classified as "special category" data (data relating to health, race, ethnicity, political opinions, religious or philosophical beliefs, trade union membership, genetic data, biometric data used for identification, sexual orientation or sex life) must be encrypted at rest and during transmission where practical to do so. Where it is not practical to encrypt the data, we will need to be able to demonstrate that adequate security is in place

6.2. The sharing of data (via digital means) within the business must only be done so through secure means

6.3. Data should only be shared by email when no other secure means are available. If data is shared via email it should be locked with a password (using a password which meets the requirements of the company's password policy). Email should always be collected and sent via a secure connection

6.4. Any devices (PCs, laptops, tablets, mobiles, etc.) that enable access to the Academy or Trust's data should be locked with appropriate password controls (in line with the company's security guidelines). This includes any personal devices authorised for used to access the data (e.g. remotely or from home)

6.5. Data should not be downloaded to local devices (PCs, laptops, tablets, mobiles, memory sticks, etc.) or to network storage devices unless authorised by the Data Protection Officer. If data is downloaded to a local device then it must only be stored for the minimal time necessary on that device and deleted once it is no longer needed on that device. An exception to this will apply where services used by the Academy or Trust require local copies of data to be stored (albeit temporarily) for those services to operate or function correctly

6.6. Data from our digital systems should not be printed out, except where absolutely necessary. If data is printed out, the printed copy of the data will be destroyed once it is no longer needed and the print out stored securely (e.g. in a locked filing cabinet) when it is not being used

6.7. Where personal data is being viewed on a device, the screen or device lock must be activated if the device is to be left unattended for any period of time – this will include laptops and computers

6.8. Employees must observe if there is a risk that any unauthorised third party would be able to view personal data whilst they, themselves, are viewing the data on a device (e.g. whilst travelling on public transport, etc.) to prevent unauthorised viewing of personal data. Screen guards should be used whenever possible, in such situations

6.9. No personal data will be transferred to personal devices, personal email or cloud storage accounts (e.g. Google Mail, Dropbox, etc.), belonging to an employee without authorisation from the Data Protection Officer

6.10. Where personal data is, with permission, downloaded, copied or printed the storage of that data should be secure at all times

6.11. Where the use of third party systems are used (and have been authorised by the Data Protection Officer), access controls will be put in place to ensure access is secure and limited to only those employees who have a need to access the data

6.12. All company systems which are used for storing or processing of personal data should be adequately and regularly backed up (in line with the company's IT policy). All backups should be encrypted and stored securely

7. Access to personal data

7.1. No employee will access data unless they are authorised to do so for the purposes of carrying out their duties as an employee

7.2. Employees will only have access to data that is required for them to carry out their duties. If they need access to data they are not currently authorised to access, they should seek access via their line manager

8. Accuracy of data and keeping it up to date

8.1. If we are told by a pupil, guardian, employee or contact that the data we hold on them is out of date or incorrect we shall make sure the incorrect data is either deleted or updated

8.2. If we are updating information about a pupil or guardian, we must do so immediately to ensure the old data is not processed in the meantime

8.3. If we have shared the data with any third party, we will immediately inform the third parties to ensure their copies of the data are updated

8.4. Where the data is stored on multiple systems we will ensure all systems' data is updated

9. Retention of data

9.1. We will only process (including store) data for as long as we have a legitimate reason to do so. We can retain data, outside our own use, where there is a legal duty for us to keep data (e.g. to meet the requirements set out by safeguarding) but any data not required must not be retained, once it is no longer needed

9.2. Where data is no longer required, and we are unable to justify a legal reason for keeping it, we will either delete the data or anonymise it, within one month for our systems. Where data is backed up or archived where it would be difficult to delete that data, we will ensure that it is not restored or easily accessible

9.3. All data will be retained in line with the timescales set in our data retention guidance

10. Subject access requests

10.1. All Data Subjects have a right to request access to the data we process and to ask how we process that data (a so called "Subject Access Request"). All subject access requests should be processed in conjunction with advice from the Data Protection Officer and in line with the Subject Access Request policy

11. Right to erasure

11.1. All requests from a Data Subject for the deletion of their data should be dealt with in consultation with the Data Protection Officer to ensure we don't delete data we have a lawful basis, or legal requirement, to continue processing

11.2. Unless where we can demonstrate otherwise, if a Data Subject requests the deletion of their data we will comply with the request, within one month of the request, and confirm to the Data Subject what data has been deleted

11.3. Where the personal data in question has been disclosed to a third party, we will notify the third party of the need for them to also erase the data

12. Right to data portability

12.1. The IT team will ensure that any systems we use that meets the requirements for a data portability option, has the data portability option available either directly to the pupil, guardian or employee or for a member of staff to activate (or to export the data into machine readable format)

12.2. Where this system is not accessible directly to the pupil, guardian or employee, all requests for an export of a data from a Data Subject will be dealt with in consultancy with the Data Protection Officer within one month of the original request

12.3. The data will be made available at least in CSV format or in a format standard that has been established between suppliers of similar systems (if available)

13. Objections to processing

13.1. Any objections to the use of data for marketing (e.g. requests to stop receiving marketing information) should be passed to the person responsible for maintaining the list. They will ensure that the details of the Data Subject are removed from any marketing lists

13.2. Any other objections are to be dealt with in consultation with the Data Protection Officer to ensure that the business does not have a lawful basis for processing

14. Third party due diligence

14.1. Where a third party is used for the processing of personal data, due diligence checks will be carried out on the third party, by the Data Protection Officer, to ensure they are data protection compliant. Such checks will include asking about how they are GDPR compliant and asking them for their GDPR statement

14.2. Contractual obligations will also be put in place with any third parties we use. Where we provide a contract to be agreed with the third party we shall ensure these contractual obligations are included in the contract either via a new contract or by an addendum to an existing contract; where we are taking a service from a third party who have their own terms of service, to which we have to agree, we must ensure that the contractual obligations are included within those terms

14.3. We will not use any third party who is unable to provide evidence of their data protection compliance or willingness to agree to the appropriate contractual terms

15. Data protection impact assessments

15.1. When new technologies, systems or processes are introduced the Data Protection Officer should be involved and carry out a Data Protection Impact Assessment to ensure the new technologies are compliant with the data protection rules and protect, by default, the privacy and rights of the Data Subjects whose data will be processed by the new technology. Consideration by the Data Protection Officer should include:

- The purposes for which personal data is being processed and the kinds of processing carried out
- An assessment of the necessity and proportionality of the processing with respect to the purposes for which it is being processed
- An assessment of the risks to the Data Subjects from the processing

- Details of steps to be taken to minimise any risk to the Data Subjects from the processing

16. Data breaches

16.1. A data breach occurs when any personal data is processed or accessed unlawfully. This may be due to a breach in security but also relates to the situation where data is accessed, destroyed or altered without the appropriate authority or shared with the wrong Data Subject

16.2. All employees have a duty to report any suspected breaches of data protection to the Data Protection Officer via their local Data Protection Champion. If an employee is in any doubt as to whether a breach has occurred, they must report it to the Data Protection Office regardless

16.3. Any data breaches will be handled by the Data Protection Officer in conjunction with the relevant Champion, in line with the Data Breach policy

17. Access by third parties

17.1. Any requests to access pupil, guardian or employee data from external parties such as the Police or a government department, should be checked by the Data Protection Officer to ensure it is lawful for us to disclose the data requested. The approach to dealing with such requests will be governed by a separate Authorised Third-Party policy

17.2. Any access by other types of third-parties, such as IT and software support should be limited to extreme situations whereby the necessary support cannot be achieved without allowing access to the system and its data. In such circumstances, these providers will be treated as third-party processors and will need to sign a data processing agreement

18. Complaints

18.1. Any complaints made to the business about the processing of personal data are to be passed, immediately, to the Data Protection Officer via the local Data Protection Champion. This includes complaints from data subjects and information requests or correspondence from the Information Commissioner's Office

19. International transfer

19.1. The company may, from time to time, transfer or process personal data outside the EU. Transfer or processing of data outside the EU will only take place when:

- The transfer is to a country that the European Commission has determined ensures an adequate level of protection for personal data

- The transfer is to a country or organisation which provides appropriate safeguards in the form of a legally binding agreement between public authorities or bodies; binding corporate rules; standard data protection clauses adopted by the European Commission; compliance with an approved code of conduct approved by a supervisory authority (e.g. the Information Commissioner's Office); certification under an approved certification mechanism (as provided for in the Regulation); contractual clauses agreed and authorised by the Information Commissioner's Office; or provisions inserted into administrative arrangements between public authorities or bodies authorised by the ICO
- The transfer is made with the informed consent of the relevant Data Subjects
- The transfer is necessary for the performance of a contract between the Data Subject and us (or for pre-contractual steps taken at the request of the Data Subject)

19.2. When data is to be transferred, or processed outside the EU for the first time the transfer must be authorised by the Data Protection Officer, this includes situations where data is processed via third-party cloud-based systems

20. Policy review

This policy will be reviewed periodically by the Data Protection Officer to ensure it is still relevant and up to date with any changes in the law, guidance or precedents set.

21. Document control

Policy updated	May 2019
Next review by DPO	May 2020