DATA PROTECTION POLICY

Date Approved by Board:	3 July 2018
Date of Review:	July 2020
Responsible Department:	Information Services
Policy Applies to:	Wellspring Trust and all Academies within the Trust

This Data Protection Policy sets out the procedures and arrangements which the Trust, its Academies, their employees and other service users must follow in order to comply with the requirements of the European General Data Protection Regulation 2018. Details pertaining to individual subject access requests are also contained within this document.

The Equality Act 2010 requires public bodies, in carrying out their functions, to have due regard to the need to:

- *eliminate discrimination and other conduct that is prohibited by the Act*
- *advance equality of opportunity between people who share a protected characteristic and people who do not share it*
- *foster good relations across all characteristics - between people who share a protected characteristic and people who do not share it.*

In the development of this policy due regard has been given to achieving these objectives.

Executive Summary

Wellspring Academy Trust will need to collect, store, process and share personal and sensitive information about its employees, pupils and other service uses. Details of applicable data and definitions are contained within this policy (see Section 3).

This policy outlines the responsibilities of all staff and governors to ensure that the Trust complies with the principles of GDPR (see Section 10). GDPR principles are contained within this policy (see Section 4).

The Trust is accountable for ensuring the implementation of appropriate technical and organisational measures that demonstrates that data processing meets the principles of GDPR.

Individuals will be informed how the Trust processes its data through privacy notices and associated policies. Internal records of processing activities will be maintained, including an Information Asset Register. This will include the Trust's legal basis for processing certain types of personal and sensitive data (see Section 8). Section 5 of this policy details the records that the Trust will maintain.

Wellspring Academy Trust registers with the ICO. (See Section 6 for an overview of the types of information with collect, process, store and share).

A Data Protection Officer (DPO) will inform and advise the Trust and its employees about its obligations to comply with GDPR and other data protection laws. The DPO will work with Information Owners (IO) and Data Protection Leads (DPL) to ensure that monitoring and compliance audits, internal data protection activities and appropriate training is available to employees.

Where explicit consent is identified as the legal basis for data processing the Trust must keep a record this for audit and compliance purposes. Consent must be a positive indication and cannot be inferred from silence, inactivity or pre-ticked boxes. It is important to note that where the legal basis of consent is used the individual can withdraw consent at any time. Where a child is under the age of 16 [or younger if the law provides it (up to the age of 13)], the consent of parents will be sought prior to the processing of their data, except where the processing is related to preventative or counselling services offered directly to a child.

All employees, pupils, service users and other individuals about whom the Trust or Academy processes personal data have the *right to be informed* about how the Trust processes their personal data (see Section 11). Individuals also have the *right to access* their personal data, where it is processed by the Trust or its Academies, whether held on computer or manually. This is process is known as a subject access request (see Section 12). Requests should be made to The Data Protection Officer via privacy@wellspringacademies.org.uk and must be responded to, within 30 days at no cost. Individuals have the right to rectification. This includes having any inaccurate or incomplete personal data rectified (see Section 13). Similarly, individuals have the right to erasure (see Section 14). This is the right to request the deletion or removal of personal data where there is no compelling reason for its continued processing. The right to restrict processing (see Section 15) allows individuals have the right to block or suppress the Trust's processing of personal data. The right to portability states that individuals have the right to obtain and reuse their personal data for their own purposes across different services (see Section 16). Individuals have the right to object to processing (see Section 17), based on legitimate interests or the performance of a task in the public interest, direct marketing or processing for purposes of scientific or historical research and statistics. Finally, individuals have the right not to be subject to automation, where a decision is based on automated processing or profiling.

The Trust operates a privacy by design approach to data processing activities. This includes conducting privacy impact assessments where existing processes are substantially changed or new processes are introduced, to determine any data protection obligations (see Section 19).

Contents

1. Statement of intent

1.1. Wellspring Academy Trust and its Academies (The Trust) will need to collect, store and process certain information about its employees, pupils and other service users, including personal and sensitive information.

1.2. The Trust will be required to share personal information about its staff or pupils with other organisations, such as the Local Authority, DfE, educational bodies, and potentially children's services.

1.3. This policy is in place to ensure that all staff and governors are aware of their responsibilities and outlines how The Trust complies with the principles of the GDPR.

1.4. Organisational methods for keeping data secure are imperative and The Trust believes that it is good practice to keep clear practical policies, backed up by written procedures.

1.5. This policy applies to all personal data held, irrespective of format (e.g. whether it is held on paper or on electronic media). The Trust is required to process personal data lawfully and therefore has taken the measures set out in this policy in order to comply with the GDPR.

1.6. In order to carry out its statutory and administrative functions, the Trust needs to collect and process personal data relating to many categories of people, including students, employees, service users and suppliers.

1.7. The Trust will only process personal data for such purposes and will disclose personal data to such third parties, as outlined in the appropriate privacy notice and in accordance with our Information Commissioner registration.

1.8. Personal data will only be retained for as long as there is a genuine requirement to do so for a specified purpose, and will not be disclosed to any unauthorised third party (unless required by law or by statutory obligation).

1.9. The aim is to provide a high standard of security for all personal data, whether it is stored electronically or in an alternative filing system. The level of security applied to sensitive personal data (as defined below) is regularly reviewed and monitored.

1.10. This Policy does not form part of an employee's formal contract of employment but it is a condition of each employee's employment with the Trust or its Academies that the employee will abide by all rules and policies. Any failure by an employee to follow this Policy may, therefore, result in disciplinary action being taken.

This policy complies with the requirements set out in the GDPR, which will came into effect on 25 May 2018. The Government has confirmed that the UK's decision to leave the EU will not affect the commencement of the GDPR.

2. Legal Framework

2.1. This policy has due regard to legislation, including, but not limited to the following:

- The General Data Protection Regulation 2018
- The Freedom of Information Act 2000
- The Education (Pupil Information) (England) Regulations 2005 (as amended in 2016)
- The Freedom of Information and Data Protection Regulations 2004
- The Trust Standards and Framework Act 1998.

2.2. This policy also has regard to the following guidance:

- ICO (2018) 'Guide to the General Data Protection Regulation (GDPR)'
- DfE (2018) Data Protection: Toolkit for schools

2.3. This policy will be implemented in conjunction with the following other policies such as:

- Data Security & Breach Management Policy.
- Data Storage, Retention & Disposal Policy.
- Freedom of Information Policy.

3. Applicable Data & Definitions

3.1. The GDPR uses a number of technical terms which are defined here:

- ***Data*** – information which is, or will be, processed automatically or manually within a relevant filing system. This includes but is not limited to written information, photographs and voice recordings. All manual data shall be deemed to be data for the purposes of this Policy;

- ***Data Subject*** – any individual who is the subject of personal data;

- ***Data Controller*** – a person or organisation (e.g. the Trust or Academy) who determines the purposes for which and the manner in which personal data is, or will be, processed;

- ***Data Processor*** – a third party person or organisation (other than an employee of the

  Data Controller) who processes data on behalf of a Data Controller;

- ***Personal Data*** – any Data relating to a living individual who can be identified from that Data or who is identifiable by combining the Data with other information available to the Data Controller (eg, phone numbers and other contact information, photographs, video or audio recordings, NHI information etc); The GDPR applies to both automated personal data and to manual filing systems, where personal data is accessible according to specific criteria, as well as to chronologically ordered data and pseudonymised data, e.g. key-coded.

- ***Sensitive Personal Data*** - is referred to in the GDPR as 'special categories of personal data', which are broadly the same as those in the Data Protection Act (DPA) 1998. These specifically include the processing of genetic data, biometric data and data concerning health matters. Personal data consisting of information regarding a Data Subject's racial or ethnic origin, political opinions, religious (or similar) beliefs, membership of a trade union, physical or mental health or condition, details of sexuality, commission or alleged commission of any offence and/or information relating to any proceedings and sentence for any committed or alleged offence of the Data Subject;

- ***Processing*** – obtaining, recording or holding data, or carrying out any operation(s) on data, including organising, adapting, altering, retrieving, disclosing, erasure, destruction and combining with other information.

4. Principles

4.1. In accordance with the requirements outlined in the GDPR, personal data will be:

- Processed lawfully, fairly and in a transparent manner in relation to individuals.

- 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.

- Adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed.

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

- 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 GDPR in order to safeguard the rights and freedoms of individuals.

- 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.

- The GDPR also requires that "the controller shall be responsible for, and able to demonstrate, compliance with the principles".

5. Accountability

5.1. Wellspring Academy Trust will implement appropriate technical and organisational measures to demonstrate that data is processed in-line with the principles set out in the GDPR.

5.2. The Trust will provide comprehensive, clear and transparent privacy policies.

5.3. Additional internal records of the Trust's processing activities will be maintained and kept up-to-date.

5.4. Internal records of processing activities will include the following:

5.4..1. Name and details of the organization
5.4..2. Purpose(s) of the processing

5.4..3. Description of the categories of individuals and personal data
5.4..4. Retention schedules
5.4..5. Categories of recipients of personal data
5.4..6. Description of technical and organisational security measures
5.4.7. Details of transfers to third countries, including documentation of the transfer mechanism safeguards in place

The Trust will implement measures that meet the principles of data protection by design and data protection by default, such as:

5.4..7. Data minimisation.
5.4..8. Pseudonymisation.
5.4..9. Transparency.
5.4..10. Allowing individuals to monitor processing.
5.4..11. Continuously creating and improving security features.
5.4..12. Data protection impact assessments will be used, where appropriate.

6. Registration Arrangement

Wellspring Academy Trust and its Academies are registered with the Information Commissioner's Office (ICO). The registration refers to the following:

6.1. *Reasons/purposes* for processing information:

We process personal information to enable us to provide education, training, welfare and educational support services, to administer Trust property; maintaining our own accounts

and records, undertake fundraising; support and manage our employees. We also use CCTV for security and the prevention and detection of crime.

6.2. *Type/classes* of information processed:

We process information relevant to the above reasons/purposes. This may include:

- Personal details
- Family details
- Lifestyle and social circumstances
- Education and employment details
- Financial details
- Goods and services
- Disciplinary and attendance records
- DBS checks
- Visual images, personal appearance and behaviour.

6.3. We also process *sensitive classes* of information that may include:

- Physical or mental health details
- Racial or ethnic origin
- Religious or other beliefs
- Trade union membership
- Sexual life
- Information about offences and alleged offences.

6.4. We process *personal information* about:

- Employees
- Pupils and their parents/carer/families
- Professional experts and advisers
- Board members, trustees and governors
- Directors
- Sponsors and supporters
- Suppliers and service providers
- Complainants and enquirers
- Customers
- Individuals captured by CCTV images.

6.5. Who the information may be *shared with*:

We sometimes need to share the personal information we process with the individual themselves and also with other organisations. Where this is necessary we are required to comply with all aspects of the GDPR. What follows is a description of the types of organisations we may need to share some of the personal information we process with for one or more reasons. Where necessary, or required, we share information with:

- Family, associates and representatives of the person whose data we are processing
- Educators and examining bodies
- Careers service
- Boards
- Local and central government
- Academy trusts
- Healthcare, social and welfare organisations

- Police forces and/or courts
- Current, past or prospective employers
- Voluntary and charitable organisations
- Business associates, professional advisers
- Suppliers and service providers
- Financial organisations
- Press and the media.

6.6. Transfers:

It may sometimes be necessary to transfer personal information overseas. When this is needed information is only shared within the European Economic Area (EEA). Any transfers made will be in full compliance with all aspects of the GDPR. Where information must be shared beyond the EEA, we ensure appropriate safeguards and assurances are taken that meet GDPR compliance standards and inform individuals through our privacy notices.

7. Data Protection Officer (DPO)

A DPO will be appointed in order to:

7.1. Inform and advise The Trust and its employees about their obligations to comply with the GDPR and other data protection laws.

7.2. Monitor The Trusts compliance with the GDPR and other laws, including managing internal data protection activities, advising on data protection impact assessments, conducting internal audits, and providing the required training to staff members.

7.3. An existing employee can be appointed to the role of DPO provided that their duties are compatible with the duties of the DPO and do not lead to a conflict of interests.

7.4. The individual appointed as DPO will have professional experience and knowledge of data protection law, particularly that in relation to the education sector.

7.5. The DPO will report to the highest level of management at the Trust, which is the Board via the appropriate Committee (e.g. Audit Committee).

7.6. The DPO will operate independently and will not be dismissed or penalised for performing their task.

7.7. Sufficient resources will be provided to the DPO to enable them to meet their GDPR obligations.

8. Lawful processing

8.1. The legal basis for processing data will be identified and documented prior to data being processed.

8.2. Under the GDPR, data will be lawfully processed under the following conditions:

8.2..1. The consent of the data subject has been obtained.

8.2..2. Processing is necessary for:

- Compliance with a legal obligation.
- The performance of a task carried out in the public interest or in the exercise of official authority vested in the controller.
- For the performance of a contract with the data subject or to take steps to enter into a contract.

- Protecting the vital interests of a data subject or another person.
- For the purposes of legitimate interests pursued by the controller or a third party, except where such interests are overridden by the interests, rights or freedoms of the data subject. (This condition is not available to processing undertaken by the school in the performance of its tasks).

8.3. Sensitive data will only be processed under the following conditions:

- Explicit consent of the data subject, unless reliance on consent is prohibited by EU or Member State law.
- Processing carried out by a not-for-profit body with a political, philosophical, religious or trade union aim provided the processing relates only to members or former members (or those who have regular contact with it in connection with those purposes) and provided there is no disclosure to a third party, without consent.
- Processing relates to personal data manifestly made public by the data subject.
- Processing is necessary for:
- Carrying out obligations under employment, social security or social protection law, or a collective agreement.
- Protecting the vital interests of a data subject or another individual where the data subject is physically or legally incapable of giving consent.
- The establishment, exercise or defence of legal claims or where courts are acting in their judicial capacity.
- Reasons of substantial public interest on the basis of Union or Member State law which is proportionate to the aim pursued and which contains appropriate safeguards.
- The purposes of preventative or occupational medicine, for assessing the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment or management of health or social care systems and services on the basis of Union or Member State law or a contract with a health professional.
- Reasons of public interest in the area of public health, such as protecting against serious cross-border threats to health or ensuring high standards of healthcare and of medicinal products or medical devices.
- Archiving purposes in the public interest, or scientific and historical research purposes or statistical purposes in accordance with article 89(1).

9. Consent

9.1. Consent must be a positive indication. It cannot be inferred from silence, inactivity or pre-ticked boxes.

9.2. Consent will only be accepted where it is freely given, specific, informed and an unambiguous indication of the individual's wishes.

9.3. Where consent is given, a record will be kept documenting how and when consent was given.

9.4. The school ensures that consent mechanisms meet the standards of the GDPR. Where the standard of consent cannot be met, an alternative legal basis for processing the data must be found, or the processing must cease.

9.5. Consent accepted under the DPA will be reviewed to ensure it meets the standards of the GDPR; however, acceptable consent obtained under the DPA will not be reobtained.

9.6. Consent can be withdrawn, by the individual, at any time.

9.7. Where a child is under the age of 16 [or younger if the law provides it (up to the age of 13)], the consent of parents will be sought prior to the processing of their data, except where the processing is related to preventative or counselling services offered directly to a child.

10. Responsibilities of Employees

The most senior post holder within the Trust service or Academy (e.g. Chief Officer or Executive Principals) are 'Information Owners' and are responsible for ensuring that the requirements of GDPR are upheld and that steps are taken to ensure that all members of staff managing and processing personal data understand that they are responsible for following good data protection practice. A Data Protection Lead (DPL) should be identified within each Academy, or service function, to provide operation support.

In addition to the obligations set out elsewhere in this policy, all employees and volunteers are responsible for:

10.1. Maintaining confidentiality and adhering to data protection legislation;

10.2. Checking that any information that they provide to the Trust or Academy, in connection with their employment, is accurate and up to date;

10.3. Informing the Trust or Academy of any changes to information which they have previously provided (e.g. change of address);

10.4. Verifying the accuracy of any information previously provided to the Trust or Academy where required from time-to-time; and

10.5. Informing the Trust or Academy of any errors in the information held by the Trust or Academy about them. The Trust or Academy cannot be held responsible for any errors in an employee's information unless the relevant employee has informed the Trust or Academy of the error.

10.6. All staff members should receive data protection training and be made aware of their responsibility to comply with data protection requirements.

If and when, as part of their responsibilities, employees collect information about other people (e.g. about colleagues, service users, pupils or details of personal circumstances), all employees must comply with the provisions of this Policy.

11. The Right to be Informed

11.1 All employees, pupils, service users and other individuals about whom the Trust or Academy processes personal data are entitled to:

- Know what information the Trust or Academy holds and processes about them and why;
- Be given a description of the recipients or classes of recipients to whom their personal data may be disclosed;
- Receive a copy of any information constituting their personal data held by the Trust or Academy (including information relating to the source of that data);
- Prevent the processing of their personal data for direct marketing purposes;
- Ask to have inaccurate personal data amended; and

- Prevent processing that is likely to cause damage or distress to themselves or anyone else.

11.2 Employees should note that unauthorised disclosure of personal data by an employee will potentially lead to disciplinary action and may be considered gross misconduct in sufficiently serious or repeated cases.

11.3 The privacy notice supplied to individuals in regards to the processing of their personal data will be written in clear, plain language which is concise, transparent, easily accessible and free of charge. (See privacy notices)

11.4 If services are offered directly to a child, the Trust will ensure that the privacy notice is written in a clear, plain manner that the child will understand.

11.5 In relation to data obtained both directly from the data subject and not obtained directly from the data subject, the following information will be supplied within the privacy notice:

11.5.1 The identity and contact details of the controller (and where applicable, the controller's representative) and the DPO.

11.5.2 The purpose of, and the legal basis for, processing the data.

11.5.3 The legitimate interests of the controller or third party.

11.5.4 Any recipient or categories of recipients of the personal data.

11.5.5 Details of transfers to third countries and the safeguards in place.

11.5.6 The retention period of criteria used to determine the retention period.

11.5.7 The existence of the data subject's rights, including the right to:

11.5.7.1.1 Withdraw consent at any time.

11.5.7.1.2 Lodge a complaint with a supervisory authority.

11.5.8 The existence of automated decision making, including profiling, how decisions are made, the significance of the process and the consequences.

11.6 Where data is obtained directly from the data subject, information regarding whether the provision of personal data is part of a statutory or contractual requirement, as well as any possible consequences of failing to provide the personal data, will be provided.

11.7 Where data is not obtained directly from the data subject, information regarding the categories of personal data that the Trust holds, the source that the personal data originates from and whether it came from publicly accessible sources, will be provided.

11.8 For data obtained directly from the data subject, this information will be supplied at the time the data is obtained.

11.9 In relation to data that is not obtained directly from the data subject, this information will be supplied:

11.9.1 Within one month of having obtained the data.

11.9.2 If disclosure to another recipient is envisaged, at the latest, before the data are disclosed.

11.9.3 If the data are used to communicate with the individual, at the latest, when the first communication takes place.

12 Rights to Access Information

12.1 Anybody whose personal data is processed by the Trust or its Academies (including but not limited to employees, pupils and service users) have the right (subject to certain statutory exemptions and restrictions) to access any personal data that is held about them (whether held on computer or manually).

12.2 Any person who wishes to exercise this right should submit the request in writing. Such requests should be immediately referred to the Data Protection Officer via privacy@wellspringacademies.org.uk . No charge will be made.

12.3 The Trust aims to comply with requests for access to personal data as quickly as possible and will in any event provide a response within 30 calendar days.

12.4 Individuals have the right to obtain confirmation that their data is being processed.

12.5 Individuals have the right to submit a subject access request (SAR) to gain access to their personal data in order to verify the lawfulness of the processing.

12.6 The Trust or its Academies will verify the identity of the person making the request before any information is supplied.

12.7 A copy of the information will be supplied to the individual free of charge; however, the Trust may impose a 'reasonable fee' to comply with requests for further copies of the same information.

12.8 Where a SAR has been made electronically, the information will be provided in a commonly used electronic format.

12.9 Where a request is manifestly unfounded, excessive or repetitive, a reasonable fee will be charged.

12.10 All fees will be based on the administrative cost of providing the information.

12.11 All requests will be responded to without delay and at the latest, within one month of receipt.

12.12 In the event of numerous or complex requests, the period of compliance will be extended by a further two months. The individual will be informed of this extension, and will receive an explanation of why the extension is necessary, within one month of the receipt of the request.

12.13 Where a request is manifestly unfounded or excessive, the Trust holds the right to refuse to respond to the request. The individual will be informed of this decision and the reasoning behind it, as well as their right to complain to the supervisory authority and to a judicial remedy, within one month of the refusal.

12.14 In the event that a large quantity of information is being processed about an individual, the Trust will ask the individual to specify the information the request is in

relation to.

13 The Right to Rectification

13.1 Individuals are entitled to have any inaccurate or incomplete personal data rectified.

13.2 Where the personal data in question has been disclosed to third parties, the Trust will inform them of the rectification where possible.

13.3 Where appropriate, the Trust or its Academies will inform the individual about the third parties that the data has been disclosed to.

13.4 Requests for rectification will be responded to within one month; this will be extended by two months where the request for rectification is complex.

13.5 Where no action is being taken in response to a request for rectification, the Trust will explain the reason for this to the individual, and will inform them of their right to complain to the supervisory authority and to a judicial remedy.

14 The Right to Erasure

14.1 Individuals hold the right to request the deletion or removal of personal data where there is no compelling reason for its continued processing.

14.2 Individuals have the right to erasure in the following circumstances:

14.2.1 Where the personal data is no longer necessary in relation to the purpose for which it was originally collected/processed

14.2.2 When the individual withdraws their consent

14.2.3 When the individual objects to the processing and there is no overriding legitimate interest for continuing the processing

14.2.4 The personal data was unlawfully processed

14.2.5 The personal data is required to be erased in order to comply with a legal obligation

14.2.6 The personal data is processed in relation to the offer of information society services to a child

14.3 The Trust and it's Academies have the right to refuse a request for erasure where the personal data is being processed for the following reasons:

14.3.1 To exercise the right of freedom of expression and information

14.3.2 To comply with a legal obligation for the performance of a public interest task or exercise of official authority

14.3.3 For public health purposes in the public interest

14.3.4 For archiving purposes in the public interest, scientific research, historical research or statistical purposes

14.3.5 The exercise or defence of legal claims

14.4 As a child may not fully understand the risks involved in the processing of data when consent is obtained, special attention will be given to existing situations where a child has given consent to processing and they later request erasure of the data, regardless of age at the time of the request.

14.5 Where personal data has been disclosed to third parties, they will be informed about the erasure of the personal data, unless it is impossible or involves disproportionate effort to do so.

14.6 Where personal data has been made public within an online environment, the Trust will inform other organisations who process the personal data to erase links to and copies of the personal data in question.

15 The Right to Restrict Processing

15.1 Individuals have the right to block or suppress the Trust's processing of personal data.

15.2 In the event that processing is restricted, the Trust and it's Academies will store the personal data, but not further process it, guaranteeing that just enough information about the individual has been retained to ensure that the restriction is respected in future.

15.3 The Trust will restrict the processing of personal data in the following circumstances:

15.3.1 Where an individual contests the accuracy of the personal data, processing will be restricted until the Trust has verified the accuracy of the data.

15.3.2 Where an individual has objected to the processing and the Trust is considering whether their legitimate grounds override those of the individual.

15.3.3 Where processing is unlawful and the individual opposes erasure and requests restriction instead.

15.3.4 Where the Trust no longer needs the personal data but the individual requires the data to establish, exercise or defend a legal claim.

15.3.5 If the personal data in question has been disclosed to third parties, the Trust will inform them about the restriction on the processing of the personal data, unless it is impossible or involves disproportionate effort to do so.

15.3.6 The Trust will inform individuals when a restriction on processing has been lifted.

16 The Right to Portability

16.1 Individuals have the right to obtain and reuse their personal data for their own purposes across different services.

16.2 Personal data can be easily moved, copied or transferred from one IT environment to another in a safe and secure manner, without hindrance to usability.

16.3 The right to data portability only applies in the following cases:

16.3.1 To personal data that an individual has provided to a controller.

16.3.2 Where the processing is based on the individual's consent or for the performance of a contract.

16.3.3 When processing is carried out by automated means.

16.4 Personal data will be provided in a structured, commonly used and machine-readable form.

16.5 The Trust will provide the information free of charge.

16.6 Where feasible, data will be transmitted directly to another organisation at the request of the individual.

16.7 The Trust is not required to adopt or maintain processing systems which are technically compatible with other organisations.

16.8 In the event that the personal data concerns more than one individual, the Trust will consider whether providing the information would prejudice the rights of any other individual.

16.9 The Trust will respond to any requests for portability within one month.

16.10 Where the request is complex, or a number of requests have been received, the timeframe can be extended by two months, ensuring that the individual is informed of the extension and the reasoning behind it within one month of the receipt of the request.

16.11 Where no action is being taken in response to a request, the Trust will, without delay and at the latest within one month, explain to the individual the reason for this and will inform them of their right to complain to the supervisory authority and to a judicial remedy.

17 The Right to Object

17.1 The Trust will inform individuals of their right to object at the first point of communication, and this information will be outlined in the privacy notice and explicitly brought to the attention of the data subject, ensuring that it is presented clearly and separately from any other information.

17.2 Individuals have the right to object to the following:

17.2.1 Processing based on legitimate interests or the performance of a task in the public interest
17.2.2 Direct marketing
17.2.3 Processing for purposes of scientific or historical research and statistics.

17.3 Where personal data is processed for the performance of a legal task or legitimate interests:

17.3.1 An individual's grounds for objecting must relate to his or her particular situation.

17.3.2 The Trust will stop processing the individual's personal data unless the

processing is for the establishment, exercise or defence of legal claims, or, where the Trust can demonstrate compelling legitimate grounds for the processing, which override the interests, rights and freedoms of the individual.

17.4 Where personal data is processed for direct marketing purposes.

17.4.1 The Trust will stop processing personal data for direct marketing purposes as soon as an objection is received.

17.4.2 The Trust cannot refuse an individual's objection regarding data that is being processed for direct marketing purposes.

17.5 Where personal data is processed for research purposes:

17.5.1 The individual must have grounds relating to their particular situation in order to exercise their right to object.

17.5.2 Where the processing of personal data is necessary for the performance of a public interest task, the Trust is not required to comply with an objection to the processing of the data.

17.6 Where the processing activity is outlined above, but is carried out online, the Trust will offer a method for individuals to object online.

18 Automated decision-making and profiling

18.1 Individuals have the right not to be subject to a decision when:

18.1.1 It is based on automated processing, e.g. profiling.

18.1.2 It produces a legal effect or a similarly significant effect on the individual.

18.2 The Trust will take steps to ensure that individuals are able to obtain human intervention, express their point of view, and obtain an explanation of the decision and challenge it.

18.3 When automatically processing personal data for profiling purposes, the Trust will ensure that the appropriate safeguards are in place, including:

18.3.1 Ensuring processing is fair and transparent by providing meaningful information about the logic involved, as well as the significance and the predicted impact.

18.3.2 Using appropriate mathematical or statistical procedures.

18.3.3 Implementing appropriate technical and organisational measures to enable inaccuracies to be corrected and minimise the risk of errors.

18.3.4 Securing personal data in a way that is proportionate to the risk to the interests and rights of the individual and prevents discriminatory effects.

18.4 Automated decisions must not concern a child or be based on the processing of sensitive data, unless:

18.4.1 The Trust has the explicit consent of the individual.

18.4.2 The processing is necessary for reasons of substantial public interest on the basis of Union/Member State law.

19 Privacy by design and privacy impact assessments

19.1 The Trust will act in accordance with the GDPR by adopting a privacy by design approach and implementing technical and organisational measures which demonstrate how the Trust has considered and integrated data protection into processing activities.

19.2 Data protection impact assessments (DPIAs) will be used to identify the most effective method of complying with the Trust's data protection obligations and meeting individuals' expectations of privacy.

19.3 DPIAs will allow the Trust to identify and resolve problems at an early stage, thus reducing associated costs and preventing damage from being caused to the Trust's reputation which might otherwise occur.

19.4 A DPIA will be carried out when using new technologies or when the processing is likely to result in a high risk to the rights and freedoms of individuals.

19.5 A DPIA will be used for more than one project, where necessary.

19.6 High risk processing includes, but is not limited to, the following:

19.6.1 Systematic and extensive processing activities, such as profiling

19.6.2 Large scale processing of special categories of data or personal data which is in relation to criminal convictions or offences

19.6.3 The use of CCTV:

19.7 The Trust will ensure that all DPIAs include the following information:

19.7.1 A description of the processing operations and the purposes

19.7.2 An assessment of the necessity and proportionality of the processing in relation to the purpose

19.7.3 An outline of the risks to individuals

19.7.4 The measures implemented in order to address risk

19.8 Where a DPIA indicates high risk data processing, the Trust will consult the ICO to seek its opinion as to whether the processing operation complies with the GDPR.

20 Publication of information

The Trust publishes a publication scheme on its website outlining classes of information that will be made routinely available, including:

- Policies and procedures
- Minutes of meetings
- Annual reports

- Financial information
- Classes of information specified in the publication scheme are made available quickly and easily on request.
- The Trust will not publish any personal information, including photos, on its website without the permission of the affected individual.
- When uploading information to the Trust website, staff are considerate of any metadata or deletions which could be accessed in documents and images on the site.

21 Conclusion

All Trust and Academy employees have a responsibility to ensure that personal data is managed and used appropriately to ensure compliance with GDPR. Any breach of this Policy and related policies by an employee may lead to disciplinary action being taken and/or criminal prosecution. Any questions or concerns about the interpretation or operation of this Policy should be referred to the Data Protection Officer.

Equality Impact Assessment

This document should be completed when developing or reviewing all policies and procedures, both at Trust level and by individual Academies

Stage 1 – The policy/procedure

Title of policy/procedure	Data Protection Policy
Department responsible for the policy/procedure	Information Services
Is it a new or previously approved policy/procedure?	Previously approved
If previously approved, what was the date?	September 2017
Name and role of assessor(s)	Jonny Wathen - CIO

Stage 2 – Further information

1. Describe the main aims, objectives and purpose of the policy/procedure	To support organisational compliance with statutory regulation such as GDPR.
2. Who is expected to benefit from this policy/procedure?	Employees, pupils, parents/carers and our supply chain.
3. Which individuals/groups/organisations have been consulted^ regarding this policy/procedure (name and roles)?	Guidance has been sought from The School Bus, DfE, Sector representatives, WAT Executive colleagues and example policies from other MATs.

^ *If any further consultation would be beneficial in ensuring that there is no adverse impact, this should be done prior to the policy/procedure being submitted to the approving body*

Stage 3 – Assessing the impact on different groups of people

In the checklist within this document please indicate whether (and how) the policy/procedure affects particular groups of people (primarily 'Equality Target Groups') compared to others. Please complete the checklist, noting the following guidance:

Positive impact: *a policy or practice where the impact on a particular group of people is more positive than for other groups, eg, accessible website design. It can also include legally permitted positive action initiatives designed to improve workforce imbalance, such as job interview guarantee schemes for disabled people.*

Negative impact*: a policy or practice where the impact on a particular group of people is more negative than for other groups, eg, where the choice of venue for a staff social occasion precludes members of a particular faith or belief group from participating.*

Neutral impact: *a policy or practice with neither a positive nor a negative impact on any group or groups of people compared to others.*

Stage 4 – Confirming completion of the Assessment

The manager responsible for developing or updating the policy/procedure is required to sign this document. The complete document (including the checklist) should then be attached to the draft policy/procedure and submitted for reference to the body which is responsible for approving it.

Stage 5 – Including a statement regarding the equality impact assessment process

The following text should be inserted (in italicised text) into the introductory section of all draft policies/procedures:

The Equality Act 2010 requires public bodies, in carrying out their functions, to have due regard to the need to:

- *eliminate discrimination and other conduct that is prohibited by the Act*
- *advance equality of opportunity between people who share a protected characteristic and people who do not share it*
- *foster good relations across all characteristics - between people who share a protected characteristic and people who do not share it.*

In the development of this policy/procedure due regard has been given to achieving these objectives.

Name:	Jonny Wathen	Job title:	Chief Information Officer
Signature:	J. Wathen	Date:	30.05.18

Confirmation that the EIA has been reviewed by a person who was not involved in the production or review of the policy:

Name	Karen Froggatt	Job title	Chief Governance Officer
Signature	K. Froggatt	Date	26/6/18

Enc: completed checklist

Equality Impact Assessment Checklist

Groups	Level of impact of the policy			Reasons / comments
	Positive	Negative	Neutral	
Equality Target Groups				
Men	Yes			A positive impact will be realised by all group in relation to personal and sensitive data collection, processing, storage and sharing.
Women	Yes			
People from black and other minority ethnic communities	Yes			
People with a disability or additional needs	Yes			
Gay, Lesbian and Bi-sexual people	Yes			
Transgender people	Yes			
Older people (50+)	Yes			
Younger people (age 17–25)	Yes			
Faith or belief groups	Yes			
Other groups				
People with mental health issues	Yes			
People with economic/social needs	Yes			