Data Protection Policy

Date Approved by Board:	September 2017
Date of Review:	May 2018 (see below)
Responsible Department:	Wellspring Trust
Policy Applies to:	Wellspring Trust and all Academies within the Trust

This Policy will be reviewed in May 2018, to take account of the introduction of the General Data Protection Regulation (GDPR) which will apply in the UK with effect from 25 May 2018.

Equality Impact Assessment: At all stages within this policy and procedure and in accordance with the Equality Act 2010, provision will be made for any reasonable adjustments to accommodate the needs of individuals.

This Data Protection Policy sets out the procedures and arrangements which the Trust, Academies within the Trust and each of their employees and other service users must follow in order to comply with the requirements of the UK Data Protection Act 1998, in particular the Eight Data Protection Principles set out in Schedule 1 to the Act.

1 Introduction

Wellspring Trust and its Academies need to process certain information about their employees, pupils and other service users for a number of purposes, such as to monitor performance, achievements and health and safety. The Trust and Academies also process personal data in order to recruit, employ and pay staff and comply with their legal obligations to funding bodies and the Government.

To comply with the Act, the Trust and its Academies are required to ensure that all personal data that they process is done so fairly, stored securely and not disclosed to any third party unlawfully. They must specifically comply with the **Data Protection Principles** which are set out in Schedule 1 to the Act. In summary these state that personal data shall:

- be processed fairly and lawfully and shall not be processed unless certain specified conditions are met;
- be obtained only for one or more specified and lawful purposes and shall not be processed in any manner incompatible with the relevant purpose(s);
- be adequate, relevant and not excessive in relation to the relevant purpose(s);
- be accurate and (where necessary) kept up to date;
- not be kept for longer than is necessary for the relevant purpose(s);
- be processed in accordance with the rights of data subjects;
- be subject to appropriate technical and organisational measures so that it is kept safe from unauthorised or unlawful processing, accidental loss, destruction and damage; and
- not be transferred to a country outside the European Economic Area, unless that country ensures an adequate level of protection in relation to personal data.

The Trust and its Academies, their employees and all others who process or use any personal data must ensure that they follow the above principles at all times, including in relation to any personal data which is in the public domain. In order to ensure that this happens, the Trust has developed this Policy.

2 Policy Statement

This Policy applies to all personal data held by the Trust and/or its Academies, irrespective of whether it is held on paper or on electronic media. The Trust and its Academies recognise the need to process personal data lawfully and therefore have taken the measures set out in this Policy in order to comply with the Act.

In order to carry out its statutory and administrative functions, the Trust and its Academies need to collect and process personal data relating to many categories of people, including students, employees, service users and suppliers - in all cases past and present.

The Trust and its Academies will only process personal data for such purposes, and disclose personal data to such third parties, in each case as have been notified to the Information Commissioner (see section 4).

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).

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.

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.

3 Definitions

The Act uses a number of technical terms which are defined here:

i. 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;

ii. Data Subject – any individual who is the subject of personal data;

iii. 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;

iv. 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;

v. 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);

vi. Sensitive Personal Data - 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;

vii. 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 Registration Arrangements

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

Reasons/purposes for processing information

We process personal information to enable us to provide education, training, welfare and educational support services, to administer school 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.

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
- vetting checks
- visual images, personal appearance and behaviour.

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.

We process personal information about:

- employees
- students and pupils
- professional experts and advisers
- members of school boards
- sponsors and supporters
- suppliers and service providers
- complainants, enquirers
- individuals captured by CCTV images.

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 Data Protection Act (DPA). 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
- school boards
- local and central government
- academy trusts
- healthcare, social and welfare organisations

 police forces, courts
 current, past or prospective employers
 voluntary and charitable organisations
 business associates, professional advisers
 suppliers and service providers
 financial organisations
 press and the media.

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 Data Protection Act.

5. Data Protection Officer

The Trust's Chief Executive Officer has overall responsibility for ensuring the Trust's and Academies' compliance with data protection legislation and has appointed a Data Protection Officer. The Data Protection Officer will lead on the Trust's overall approach to data protection.

The Data Protection Officer is responsible for:

- Ensuring compliance with data protection principles
- Developing and progressing a data protection action plan
- Ensuring that notification of processing of personal data and sensitive personal data to the ICO is up to date
- Providing guidance and advice to staff members in relation to compliance with legislative requirements.

Any queries relating to this Policy or the handling of personal data should be referred to the Data Protection Officer.

6. Responsibilities of Employees

The Principal of each Academy is responsible for ensuring that the requirements of the Data Protection Act are upheld at their Academy 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.

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

- Maintaining confidentiality and adhering to data protection legislation;
- Checking that any information that they provide to the Trust or Academy in connection with their employment is accurate and up to date;
- Informing the Trust or Academy of any changes to information which they have previously provided (e.g. change of address);
- Verifying the accuracy of any information previously provided to the Trust or Academy where required from time to time; and
- 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.

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 (including but not limited to the provisions of Appendix 1).

7. Notification of Data Held and Processed

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.

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.

All personal data should:

- in the case of manual personal data, be kept in a locked filing cabinet or locked drawer; and
- in the case of electronic personal data:

    1. where the personal data is stored on equipment which is physically installed at the Trust or Academy premises, be password protected; and
    2. where the personal data is stored on any portable equipment or device (including but not limited to USB drives, CD-ROMs, DVD- ROMs and laptop computers), only be stored on such equipment/device where the equipment/device has been encrypted (password protection is not sufficient), with CD-ROMs and DVD-ROMs being destroyed when no longer required, provided that personal data should never be copied onto any portable equipment or device without specific authorisation from the Data Protection Officer.

If any portable equipment or device is used to store personal data, the equipment/device should be kept in a secure location at all times (e.g. it should never be left unattended in a vehicle). In the event that any such equipment or device is lost or stolen, or there is concern that it may have been accessed by an unauthorised person or otherwise compromised, this must be reported to the Data Protection Officer immediately.

Employees should not store or transfer personal data using any cloud storage or other file sharing system (such as Dropbox, Google Drive, Sky Drive or iCloud) without specific authorisation from the Data Protection Officer. Such systems may involve the transfer of

personal data outside the European Economic Area and potentially breach the eighth data protection principle contained within the Act.

Employees should be aware that there is no specific exemption in the Act which applies to information in the public domain, and that the Act and the eight data principles (such as the obligation to process personal data fairly and lawfully) also apply to information in the public domain.

Personal data may only be transferred to a third party data processor if the data processor agrees in writing to comply with the Trust's procedures and policies, or puts in place adequate measures itself.

8. Rights to Access Information

Anybody whose personal data is processed by the Trust or Academy (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).

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. No charge will be made for the first occasion that access is requested by any particular individual, but the Trust reserves the right to make a charge of £10 per each subsequent request.

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 40 calendar days.

9. Data Subject Consent

In many cases, the Trust or Academy can only process personal data with the consent of the relevant individual. An individual's agreement to the Trust or Academy processing certain types of their personal data is a condition of employment for employees.

As part of the Trust's recruitment process, prospective employees are required to give their consent to the processing of their personal data (including certain types of sensitive personal data) by completing an application form and signing against both the data protection declaration and the safeguarding children / vulnerable adults section. A refusal to sign can result in non-consideration of the application.

The Trust's contract of employment, which is required to be signed by employees, includes a data protection statement that records the employee's consent to the Trust or Academy collecting, holding and processing their personal data and certain sensitive personal data for specified reasons (such as to comply with legal obligations placed on the Trust as an employer, and for administrative purposes such as arranging payment of wages.

10. Processing Sensitive Information

Sometimes it is necessary for the Trust or Academy to process a person's sensitive personal data, including but not limited to information about a person's health, criminal convictions, race, gender and family details. This may be for health and safety reasons or where required by other Trust policies, such as the Equality and Diversity Policy. Because of the sensitive nature of the information and the potential concern and/or distress which disclosing such information may cause to individuals, employees, pupils and service users will be asked to give express consent for the Trust to do this (as indicated in section 9 above).

11. Retention of Data

The Trust or Academy will keep some types of information for longer than others. By law, personal data (whether about employees, pupils, service users or any other individual) must only be retained for as long as there is a genuine need for it and cannot be stored indefinitely.

All employees are required to follow the Trust's archiving guidelines and retention times as set out in Appendix 2.

12. Disposal of Data

When personal data is no longer required or has passed its retention date, it must be securely deleted and/or destroyed (as the case may be). In the case of manual records (e.g. paper files), all such records must be securely shredded.

Personal data which is held electronically must be permanently deleted, with particular care taken that any 'hidden' data cannot be recovered.

13. Closed Circuit Television

The Trust or Academy has installed CCTV systems at a number of its premises in order to protect the integrity of property and the security, health and safety of its employees, pupils, service users and other visitors. Using CCTV acts as a deterrent to potential trespassers, thieves and vandals and those who choose to breach health and safety rules and other procedures.

Only authorised personnel have routine access to live and recorded images generated by the CCTV systems, although images will be provided to law enforcement authorities where appropriate. The Trust or Academy may use recorded images as evidence in misconduct and performance related investigations, as well as in disciplinary and court proceedings.

14. Data breaches

In the event of any breaches of sensitive data, the data subject will be informed as appropriate, as with the ICO, further to which the matter will be reported to the Trust's Audit Committee.

15. Conclusion

All Trust and Academy employees have a responsibility to ensure that personal data is managed and used appropriately to ensure compliance with the Act. Any breach of this Policy 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.

16. List of Appendices

Appendix 1 - Employee Guidelines for Processing Personal Data (including checklist for recording data)

Appendix 2 - Guidelines for Retention of Records Containing Personal Data.

Appendix 1

Employee Guidelines for Processing Personal Data

1. Many employees will be required as part of their duties to collect, hold and process personal data (including sensitive personal data) for which Wellspring Trustor or each of its Academies is the Data Controller. This largely relates to employee records and / or information about pupils and other service users. Employees must not access such information unless they have been given permission to do so.

   The information that employees deal with on a day-to-day basis regarding students will include:

   - General personal details (such as name and address);
   - Details about pupil attendance and progress;
   - Notes of personal supervision, including matters about behaviour and discipline.

   Personal data should only be collected to the extent that it is required for the specific purpose notified to the individual. Any information which is not necessary for that purpose should not be collected.

2. An individual's sensitive personal data (as defined in section 3 above) should only be collected and processed with the relevant individual's consent except in the case of a genuine medical emergency. Such information should only be recorded on the Trust's r Academy's relevant standard form(s) (e.g. application form or approved questionnaires).

   Examples of where sensitive personal data may be required in relation to pupils include (eg): recording information about dietary needs or for religious or health reasons prior to taking students on a school trip.

3. All employees have a duty to make sure that they comply with the data protection principles contained within the Act, which are summarised in section 1 of this Policy. In particular, employees must ensure that records are and remain:

   - Accurate;
   - Up-to-date;
   - Processed fairly and lawfully; and
   - Kept and disposed of safely, and in accordance with this Policy.

   Inaccurate or out-of-date information should be destroyed.

4. Personal data must not be collected for one purpose and then used for another purpose. If it becomes necessary to change the purpose for which the information is processed, the individual must be informed of the new purpose before any processing occurs.

5. Employees must not disclose personal data to any other employee or pupil except with the agreement of the Data Protection Officer, or where done so in accordance authorised policies and procedures.

6. Information about the Trust's or Academy's employees, pupils, service users and other individuals must not be disclosed to any third party or to the person to whom it relates except in accordance with this Policy and the Trust's or Academy's authorised procedures. In the event of a request being received from a third party for disclosure of, or to inspect, information relating to any individual (including but not limited to employees, pupils and service users) this should be referred to the Data Protection Controller, regardless of the identity of the requestor (including where the requestor is the police or any other government agency or public authority).

7. Any requests for references must be referred to the Chief Human Resources Officer.

8. Personal comments and opinions in correspondence and other documents should be avoided wherever possible as individuals have the right to request copies of all the personal data that the Trust or Academy holds about them, including such written comments and opinions. All email messages may be disclosed in legal proceedings in the same way as paper documents, and should be treated as potentially retrievable even after they have been deleted.

9. Personal data should not be printed off unless absolutely necessary. In all cases, manual records must be stored securely.

10. Personal data relating to employees, pupils, service users or others should not be left where unauthorised people can see it (e.g. computer terminals visible to people other than authorised employees should not be left unattended or made visible to third parties, except as required to carry out the transaction in question).

11. Before processing any personal data, all employees should consider the following checklist:

- Do you really need to record the information?
- Is the information 'standard' or is it 'sensitive'?
- If it is sensitive, do you have the data subject's express consent?
- Has the data subject been told that this type of data will be processed?
- Are you authorised to collect/store/process the data?
- If yes, have you checked with the data subject that the data is accurate?
- Are you sure that the data is secure?
- If you do not have the data subject's consent to process, are you satisfied it is in the legitimate interests of the data subject or the Trust or Academy to collect and retain the data?

Appendix 2

Guidelines for Retention of Records Containing Personal Data

Type of Data	Retention Period	Reason
Personnel Files; training records; notes of grievance and disciplinary hearings	6 years from the end of employment	Provision of references and limitation period for litigation
Staff Application forms; interview notes	6 months from the date of the interviews	Limitation period for litigation
Facts relating to redundancies (less than 20)	3 years from the date of redundancies	Limitation period for litigation
Facts relating to redundancies (20 or more)	12 years from the date of redundancies	Limitation period for litigation
Income Tax and NI returns; correspondence with Tax Office	3 years after the end of the financial year to which the records relate	Income Tax (Employment) Regulations 1993
Statutory Maternity Pay records and calculations	3 years after the end of the financial year to which the records relate	Statutory Maternity Pay (General) Regulations 1986 and subsequent amendments
Statutory Sick Pay records and calculations	3 years after the end of The financial year to which the records relate	Statutory Sick Pay (General) Regulations 1982
Wages and salary records	6 years from the last date of employment	Taxes Management Act 1970
Records and reports of accidents	3 years after the date of the last entry	Social Security (Claims And Payments) Regulations 1979; RIDDOR 1995
Health Records	During Employment	Management of Health and Safety at Work Regulations
Health Records where reason for termination of employment is concerned with health, including stress related illness	3 years	Limitation period for personal injury claims
Medical Records kept by reason of the Control of Substances Hazardous to Health (COSHH)	40 years	COSHH Regulations 1999
European Regional Development Fund (ERDF) Project Documentation	15 years from the start date of the project. This may be extended by the Department for Communities and Local Government in the year 2025	Audit requirements

European Social Fund (ESF) Project Documentation	All learner data and documents will be retained until the end of the document retention period for the 2007 to 2013 ESF programme (at least 31 December 2022)	SFA ESF Audit Requirements
Pupil records including academic achievements and conduct	6 years from the last day of the course (course work – 3 years); 10 years with the consent of the student for personal and academic references. Certain personal data may be held in perpetuity	Limitation period for negligence