Management of Information Policy Suite

Responsibility for approval: Directors Group
Date of approval: November 2023

Contents Page

Table of Contents

1. Policy Statement

1.1. We are an ambitious and inclusive Trust of schools strengthening our communities through excellent education. We are committed to providing excellent education for every child, every day, and aim to strengthen and work with our communities to ensure confident compliance.

1.2. This policy is based on our values of collaboration and building trust; it sets out the Trust's framework to ensure compliance with the UK GDPR Data Protection Principles, its retention of personal data and in providing a right of access to official information in line with what is permitted by the Freedom of Information Act.

2. Definitions

2.1. For the purpose of this document the Ted Wragg Multi Academy Trust is referred to as **the Ted Wragg Trust or TWT** or **the Trust.**

2.2. UK GDPR defines "personal data" as any information relating to an identified or identifiable natural person; an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier, or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural, or social identity of that natural person.

2.3. Special Category data was previously termed "Sensitive Personal Data". Special Category Data is similar by definition and refers to data concerning an individual Data Subject's racial or ethnic origin, political or religious beliefs, trade union membership, physical and mental health, sexuality, biometric or genetic data and personal data relating to criminal offences and convictions.

2.4. The Data Controller is the person or organisation that determines the purposes and the means of processing of personal data.

2.5. The Data Processor is the person or other body, other than an employee of the data controller, who processes personal data on behalf of the Data Controller.

2.6. The Data Subject is the identified or identifiable individual whose personal data is held or processed.

2.7. Processing data involves any activity that involves the use of personal data. This includes but is not limited to: obtaining, recording or holding data or carrying out any operation or set of operations on that data such as organisation, amending, retrieving, using, disclosing, erasing or destroying it. Processing also includes transmitting or transferring personal data to third parties.

2.8. Automated Processing - Any form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to an individual, in particular to analyse or predict aspects concerning that individual's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements. An example of automated processing includes profiling and automated decision making. Automatic decision-making is when a decision is made which is based solely on automated processing (without human intervention) which produces legal effects or significantly affects an individual. Automated decision making is prohibited except in exceptional circumstances.

2.9. Biometric data - Personal information about an individual's physical or behavioural characteristics that can be used to identify that person; this can include their fingerprints, facial shape, retina and iris patterns and hand measurements

2.10. Data Protection Impact Assessments - DPIAs are a tool used to identify risks in data processing activities with a view to reducing them.

2.11. Criminal Records Information – This refers to personal information relating to criminal convictions and offences, allegations, proceedings and related security measures.

2.12. Trust Information Asset Register – This refers to the data mapping process completed by the Trust on the Judicium platform to record what data is processed, why and how it is stored.

3. Legal Framework

3.1 This policy has due regard to the following legislation and guidance, including, but not limited to, the following:

- The Management of Information Policy Suite meets the requirements of UK General Data Protection Regulation (UK GDPR).

- The Data Protection, Privacy and Electronic Communications (Amendments etc) (EU Exit) Regulations 2020 has replaced the EU Legislation.
- The Data Protection Act (DPA 2018).
- The Freedom of Information Act 2000 (FOI) which came into full force on January 1 2005
- Protection of Freedoms Act 2012, sections 26 to 28 (biometric data)
- Reflects the ICO guidance for the use of surveillance cameras and personal information and is based on the principles of UK data protection law.
- Limitation Act 1980

4. Scope and purpose

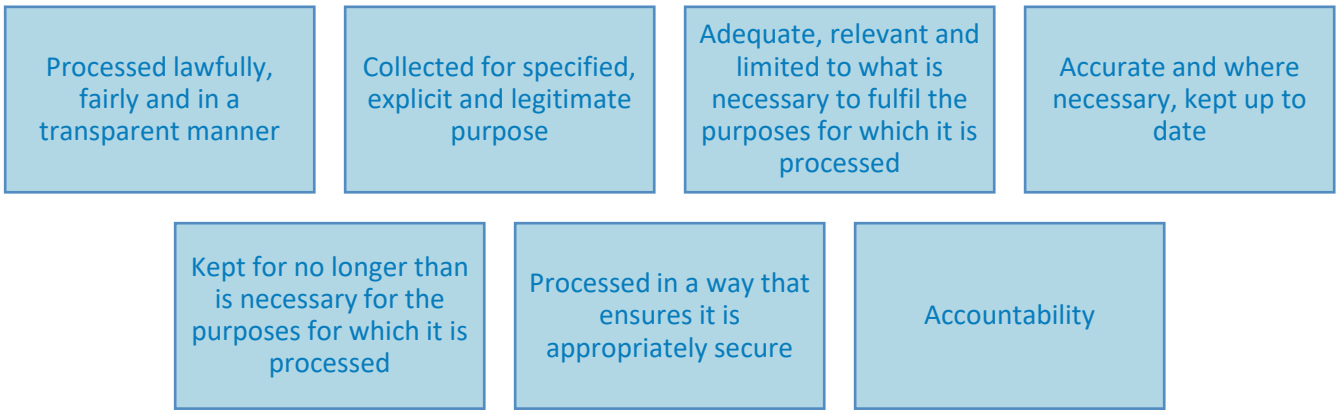
4.1. This policy suite sets out the procedures that are to be followed when dealing with personal data and information requests. The procedures and principles set out herein must be followed at all times by the Trust, its employees, agents, contractors, or other parties working on behalf of the Trust.

4.2. This policy outlines how information will be processed, stored, accessed, monitored, retained and disposed of, to meet the Trust's statutory requirements to comply with the UK GDPR, Freedom of Information Act and other relevant statutory legislation.

4.3. This policy suite sets out the Framework for how the Ted Wragg Trust manages its obligations in terms of responding to written requests from the public and publishing certain information about its activities through the Freedom of Information Act Publication Scheme.

5. The Data Protection Principles

5.1. The UK GDPR is based on data protection principles that the Trust and its schools must comply with.



5.2. All staff are responsible for collecting, storing and processing personal data in accordance with this policy and the data protection principles.

5.3 All staff must comply with the relevant processes to ensure consents have been given, report any breaches via the process outlined in this policy, and liaise with the school's Compliance Lead to seek guidance from the Data Protection Officer (DPO) when required.

6. The Data Protection Officer

6.1. The Trust has appointed an external Data Protection Officer (DPO) Service, Judicium to fulfil the legal requirement for oversight of the compliance with data protection laws, these policies and support with developing guidance as required.

6.2. Our DPO contact details are dataservices@judicium.com

Judicium Education
72 Cannon Street,
London, EC4N 6AE

7. The School's Compliance Lead

7.1. Each school appoints a Compliance Lead who manage the data protection on a day to day basis, they provide the link between the DPO and the school, are part of a Trust wide Compliance Leads network to develop confidence in compliance and liaise with the QA & Compliance Coordinator in the Trust.

8. Collecting Personal Data

8.1 Lawful, Fair, and Transparent Data Processing: UK GDPR seeks to ensure that personal data is processed lawfully, fairly, and transparently, without adversely affecting the rights of the person. UK GDPR states that processing of personal data shall be lawful if at least one of the following applies:

a. **Consent** - the data subject has given consent to the processing of his or her personal data for one or more specific purposes;

b. **Contractual** - processing is necessary for the performance of a contract to which the data subject is a party or in order to take steps at the request of the data subject prior to entering into a contract;

c. **Legal Obligation** - processing is necessary for compliance with a legal obligation to which the controller is subject;

d. **Vital Interests** - processing is necessary to protect the vital interests of the data subject or of another natural person;

e. **Public Interest** - processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller;

f. **Legitimate Interests** - processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child.

8.2 Processed for Specified, Explicit and Legitimate Purposes: The Trust only processes personal data for the specific purposes set out in the Trust Information Asset Register (or for other purposes expressly permitted by UK GDPR). The purposes for which we process personal data will be informed to data subjects through the publication of Privacy Notices.

8.3 Adequate, Relevant and Limited Data Processing: The Trust will only collect and process personal data for and to the extent necessary for the specific purpose(s) informed to data subjects as under Section 8.2, above.

8.4 Accuracy of Data and Keeping Data Up to Date: The Trust shall ensure that all personal data collected and processed is kept accurate and up-to-date. The accuracy of data shall be checked when it is collected and at regular intervals thereafter. Where any inaccurate or out-of-date data is found, all reasonable steps will be taken without delay to amend or erase that data, as appropriate.

8.5 Timely Processing: The Trust shall not keep personal data for any longer than is necessary taking into account the purposes for which that data was originally collected and processed. When the data is no longer required, all reasonable steps will be taken to erase or will be securely disposed without delay.

8.6 Secure Processing: The Trust shall ensure that all personal data collected and processed is kept secure and protected against unauthorised or unlawful processing and against accidental loss, destruction or damage.

8.7 Accountability:

8.7.1 The Trust's Executive Director of People, Strategy & IT holds accountability for Data Protection through an outsourced Data Protection Officer (DPO) service.

8.7.2 The Trust shall keep written internal record of all personal data collection, holding, and processing, in the form of an information asset register, which shall incorporate the following information:

a. The name and details of the Trust, its Data Protection Officer, and any applicable third-party data controllers
b. The purposes for which the Trust processes personal data
c. Details of the categories of personal data collected, held, and processed by the Trust; and the categories of data subject to which that personal data relates
d. Details (and categories) of any third parties that will receive personal data from the Trust
e. Details of any transfers of personal data to non-EEA countries including all mechanisms and security safeguards
f. Details of how long personal data will be retained by the Trust

9. Data Protection Impact Assessments (DPIAs)

9.1 The Trust shall carry out Data Protection Impact Assessments (DPIAs) when and as required under UK GDPR. DPIAs shall be overseen by the Trust's DPO Service and shall address the following areas of importance:

a. The purpose(s) for which personal data is being processed and the processing operations to be carried out on that data;
b. Details of the legitimate interests being pursued by the Trust;
c. An assessment of the necessity and proportionality of the data processing with respect to the purpose(s) for which it is being processed;
d. An assessment of the risks posed to individual data subjects; and
e. Details of the measures in place to minimise and handle risks including safeguards, data security, and other measures and mechanisms to ensure the protection of personal data, sufficient to demonstrate compliance with UK GDPR.

9.2 The Quality Assurance & Compliance Lead, will liaise with the DPO Service, IT and the relevant Trust or school staff leading on the data processing mechanism.

9.3 DPIAs will be carried out on any data collection process that includes special category data, e.g. biometric data.

10. The Rights of Data Subjects

10.1 UK GDPR sets out the following rights applicable to data subjects:

a. The right to be informed
b. The right of access
c. The right to rectification
d. The right to erasure (also known as the 'right to be forgotten')
e. The right to restrict processing
f. The right to data portability
g. The right to object
h. Rights with respect to automated decision-making and profiling

10.2 Keeping Data Subjects informed via **Privacy Notices** published on the Trust and schools' websites.

11. Sharing personal data

11.1 We will not normally share personal data with anyone else without consent, however, there are certain circumstances where the Trust or one of its schools may be required to do so. These include but are not limited to, situations where:

a. There is an issue with a student or parent/carer that puts the safety of our staff at risk
b. Our suppliers or contractors need data to enable us to provide services to our staff and students. We will only appoint suppliers or contractors which can provide sufficient guarantees that they comply with UK data protection law, and ensure we only share data that is needed to carry out their service.
c. Law enforcement and government bodies where we are legally required to share personal data.
d. Emergency services, local authorities and external agencies to help them respond to situations where support is required that affects any of our students or staff.

e. Any data transferred internationally, we will do so in accordance with the UK data protection law.

12. Subject Access Requests (SAR)

12.1 A person may make a **subject access request (SAR)** at any time to gain access to personal information that the school and/or Trust holds about them as outlined in **Appendix B**. ***There is a link on each school website to complete a SAR request*.**

12.2 All SARs received must be forwarded to the relevant Headteacher. The Compliance Lead will liaise with the relevant parties to obtain the information and with the DPO before sending to the data subject.

12.3 The response time is normally within one month of receipt, this can be extended by up to two months in the case of complex and/or size of request. Any requests received within 15 working days of the end of term or half term may have a longer response time, in such cases the data subject will be informed of the need for the extension.

12.4 The Trust does not charge a fee for handling of normal SARs. The Trust reserves the right to charge reasonable fees for additional copies of information that has already been supplied to a data subject, and for requests that are manifestly unfounded or excessive, particularly where such requests are repetitive.

12.5 Staff members can find a detailed guidance noted on the process in Section 3 of the Compliance Lead Guide on Management of Information.

13. Children and Subject Access Requests

13.1 Personal data about a child belongs to that child, and not the child's parents or carers. For a parent or carer to make a subject access request on behalf of their child, the child must either be unable to understand their rights and the implications of a subject access request or have given their consent.

13.2 Children aged 12 and above are generally regarded to be mature enough to understand their rights and the implications of a subject access request. Therefore, subject access requests from those with parental responsibility for students within the trust aged 12 and above may not be granted without the express permission of the student.

13.3 Children below the age of 12 are generally not regarded to be mature enough to understand their rights and the implications of a subject access request. Therefore, subject access requests from those with parental responsibility for students within our trust aged under 12 will in general be granted without requiring the express permission of the student.

These are not fixed rules and a student's ability to understand their rights will always be judged on a case by case basis.

14. Parental requests to see the Educational Record

14.1 Parents have no automatic right of access to the educational record in their child's setting. The Trust and its schools will treat this is the same as a subject access request and apply the same response timelines.

14.2 The school may charge a fee to cover the cost of supplying the educational record.

14.3 There are certain circumstances in which this request would be denied, such as if releasing the information might cause serious harm to the physical or mental health of the student or another individual, or would mean releasing exam marks before officially announced.

15. Biometric Data

15.1 All biometric is considered to be special category data under the UK General Data Protection Regulation (UK GDPR). This means the data is more sensitive and requires additional protection as this type of data could create more significant risks to a person's fundamental rights and freedoms.

15.2 This policy complies with the Protection of Freedoms Act 2012 (Sections 26-28), the Data Protection Act 2018 and the UK GDPR.

15.3 Biometric data is special category data, and the school must have a separate condition for processing special category data.

15.4 When processing biometric data, the schools must obtain explicit consent (which satisfies the fair processing conditions for personal and special category data). Consent is obtained from the parents via the school prior to any implementation. Appendix D sets out the process for consent and any withdrawal or refusal rights.

15.5 Retention of biometric data how it will be stored and deleted is set out in our Retention Schedule (Appendix C).

16. CCTV

16.1 We use CCTV in various locations around some of our school sites to ensure the site remains safe. We will adhere to the ICO's code of practice for the use of CCTV.

16.2 The school will have carried out a DPIA risk assessment prior to installing any CCTV and this informs the school's use of CCTV. Further details on the school's management of CCTV are set out in Appendix E.

16.3 We do not need to ask individuals' permission to use CCTV, but we make it clear where individuals are being recorded. Security cameras are clearly visible and accompanied by prominent signs explaining that CCTV is in use.

16.4 Any enquiries about the CCTV system should be directed to the Headteacher of the school.

17. Photographs and videos

17.1 Details of written consent and their use is detailed in our Photographic & Digital Images Policy published on the Trust and schools' websites.

18. Direct Marketing

18.1 The School are subject to certain rules and privacy laws when marketing. For example, a data subject's prior consent will be required for electronic direct marketing (for example, by email, text or automated calls).

18.2 The School will explicitly offer individuals the opportunity to object to direct marketing and will do so in an intelligible format which is clear for the individual to understand. The School will promptly respond to any individual objection to direct marketing.

19. Rectification of personal data

19.1 If a person informs the Trust that personal data held by the Trust is inaccurate or incomplete, requesting that it be rectified, the personal data in question shall be rectified, and the data subject informed of that rectification, within one month of receipt the data subject's notice (this can be extended by up to two months in the case of complex requests, and in such cases the data subject shall be informed of the need for the extension).

20. Erasure of personal data

20.1 Data subjects may request that the Trust erases the personal data it holds about them in the following circumstances:

a. It is no longer necessary for the Trust to hold that personal data with respect to the purpose for which it was originally collected or processed
b. The data subject wishes to withdraw their consent to the Trust holding and processing their personal data (and there is no overriding legitimate interest to allow the Trust to continue doing so)
c. The data subject objects to the Trust holding and processing their personal data (and there is no overriding legitimate interest to allow the Trust to continue doing so)
d. The personal data has been processed unlawfully
e. The personal data needs to be erased in order for the Trust to comply with a particular legal obligation

20.2 Unless the Trust has reasonable grounds to refuse to erase personal data, all requests for erasure shall be complied with, and the data subject informed of the erasure, within one month of receipt of the person's request (this can be extended by up to two months in the case of complex requests, and in such cases the data subject

shall be informed of the need for the extension).

21. Restriction of personal data processing

21.1 A person may request that the Trust ceases processing the personal data it holds about them. Unless the Trust has reasonable grounds to refuse, all requests shall be complied with and shall retain only the amount of personal data pertaining to that data subject that is necessary to ensure that no further processing of their personal data takes place.

22. Data portability

21.1 Where a person has given their consent to the Trust to process their personal data in such a manner or the processing is otherwise required for the performance of a contract between the Trust and the data subject, data subjects have the legal right under UK GDPR to receive a copy of their personal data and to use it for other purposes (namely transmitting it to other data controllers, e.g. other organisations).

21.2 Where technically feasible, if requested, personal data shall be sent directly to another data controller.

21.3 All requests for copies of personal data shall be complied with within one month of the data subject's request (this can be extended by up to two months in the case of complex requests in the case of complex or numerous requests, and in such cases the data subject shall be informed of the need for the extension).

23. Objections to personal data processing

22.1 Where a person objects to the Trust processing their personal data based on its legitimate interests, the Trust shall cease such processing forthwith, unless it can be demonstrated that the Trust's legitimate grounds for such processing override the data subject's interests, rights and freedoms; or the processing is necessary for the conduct of legal claims.

22.2 Where a person objects to the Trust processing their personal data for direct marketing purposes, the Trust shall cease such processing forthwith.

22.3 Where a data subject objects to the Trust processing their personal data for scientific and/or historical research and statistics purposes, the data subject must, under UK GDPR, 'demonstrate grounds relating to his or her particular situation'. The Trust is not required to comply if the research is necessary for the performance of a task carried out for reasons of public interest.

24. Automated decision-making

23.1 In the event that the Trust uses personal data for the purposes of automated decision-making and those decisions have a legal (or similarly significant effect) on data subjects, a person has the right to challenge such decisions under UK GDPR, requesting human intervention, expressing their own point of view, and obtaining an explanation of the decision from the Trust.

23.2 This right does not apply in the following circumstances:

a. The decision is necessary for the entry into, or performance of, a contract between the Trust and the data subject
b. The decision is authorised by law; or
c. A person has given their explicit consent.

25. Profiling

24.1 Where the Trust uses personal data for profiling purposes, the following shall apply:

a. Clear information explaining the profiling will be provided, including its significance and the likely consequences;
b. Appropriate mathematical or statistical procedures will be used;
c. Technical and organisational measures necessary to minimise the risk of errors and to enable such errors to be easily corrected shall be implemented; and
d. All personal data processed for profiling purposes shall be secured in order to prevent discriminatory effects arising out of profiling.

26. Data protection measures

25.1 The Trust shall ensure that the following measures are taken with respect to the collection, holding and processing of personal data:

a. All employees, agents, contractors, or other parties working on behalf of the Trust shall be made fully aware of both their individual responsibilities and the Trust's responsibilities under UK GDPR and under this Policy, and shall be provided with a copy of this Policy;
b. Only employees, agents, sub-contractors, or other parties working on behalf of the Trust that need access to, and use of, personal data in order to carry out their assigned duties correctly shall have access to personal data held by the Trust;
c. All employees, agents, contractors, or other parties working on behalf of the Trust handling personal data will be appropriately trained to do so;
d. Methods of collecting, holding and processing personal data shall be regularly evaluated and reviewed;
e. Where any agent, contractor or other party working on behalf of the Trust handling personal data fails in their obligations under this Policy that party shall indemnify and hold harmless the Trust against any costs, liability, damages, loss, claims or proceedings which may arise out of that failure.

27. Employee Obligations

26.1 Employees may have access to the personal data of other members of staff, suppliers, parents or pupils of the Trust and its schools in the course of their employment or engagement. If so, the Trust expects those employees to help meet the Trust's data protection obligations to those individuals.

28. Records Management

27.1 Records management is defined as a field of management responsible for the efficient and systematic control of the creation, receipt, maintenance, use, distribution, storage and disposal of records.

27.2 Records management helps to:

a. Ensure that the Trust conducts itself in an efficient and accountable manner
b. Meet legislative and regulatory requirements
c. Support and document policy formation and decision-making
d. Facilitate the effective performance of activities and delivery of services throughout the Trust
e. Provide continuity in the event of a disaster
f. Protect the interests of the Trust in the event of litigation or otherwise
g. Establish and maintain the Trust's cultural identity and institutional memory

27.3 The Trust has a corporate responsibility to maintain its records and records management systems in accordance with legislation:

a. Each school within the Trust is individually responsible for the management of the records generated by its activities and to ensure all activities comply with this policy.
b. Individual members of staff should ensure that records, for which they are responsible, are maintained and disposed of in accordance with this policy.
c. Records Management Good Practice Guidance is published in Section 7 of the Compliance Lead Guide for Management of Information.

27.4 **Archive and disposal:** Documents should be archived in accordance with the Retention Schedule in **Appendix C**.

a. Personal data that is no longer needed will be disposed of securely. Personal data that has become inaccurate or out of date will also be disposed of securely, where we cannot or do not need to rectify or update it
b. Where we use a third party to safely dispose of records on the school's behalf, we will require the third party to provide sufficient guarantees that it complies with data protection law.

27.5 The Trust shall ensure compliance with the operational measures outlined in Section 7 on records management in the Compliance Lead's Management of Information Guide**.**

29. Personal data breaches

28.1The Trust and its schools will make all reasonable endeavours to ensure that there are no personal data breaches.

28.2 In the unlikely event of a suspected data breach, we will advise our DPO and follow the procedure set out in the Section 2 on records management in the Compliance Lead's Guide to Management of Information.

28.3 When appropriate, we will report the data breach to the ICO within 72 hours after becoming aware of it. Such breaches in a school context may include, but are not limited to:

a. A non-anonymised dataset being published on the school website which shows the exam results of students eligible for the pupil premium
b. Safeguarding information being made available to an unauthorised person
c. The theft of a school laptop containing non-encrypted personal data about students

28.4 A review of the incident will take place and reported onto the Trust's termly breach report and presented with any recommendations for changes to systems, policies and procedures.

28.5 The termly report will be presented to the Trust Board's Education Committee.

30. Freedom of Information Publication Scheme

29.1 The Trust has adopted the Model Publication Scheme for Schools approved by the Information Commissioner and is held in **Appendix A**. This publication scheme commits the Trust to making information available to the public as part of its normal business activities. The information covered is included in classes of information, where this information is held by the Trust.

29.2 The scheme commits the Trust to:

a. Proactively publish or otherwise make available as a matter of routine, information, which is held by the Trust and falls within the classifications
b. Specify the information which is held by the Trust and falls within the classifications
c. Proactively publish or otherwise make available as a matter of routine, information in line with the statements contained within this scheme
d. Produce and publish the methods by which the specific information is made routinely available so that it can be easily identified and accessed by members of the public
e. Review and update on a regular basis the information the Trust makes available under this scheme
f. Produce a schedule of any fees charged for access to information which is made proactively available;
g. Make this publication scheme available to the public
h. Publish any dataset held by the Trust that has been requested, and any updated versions it holds, unless the Trust is satisfied that it is not appropriate to do so; to publish the dataset, where reasonably practicable, in an electronic form that is capable of re-use; and, if any information in the dataset is a relevant copyright work and the Trust is the only owner, to make the information available for re-use under the terms of the Re-use of Public Sector Information Regulations 2015, if they apply, and otherwise under the terms of the Freedom of Information Act section 19. The term 'dataset' is defined in section 11(5) of the Freedom of Information Act. The term 'relevant copyright work' is defined in section 19(8) of that Act.

31. Responding to Freedom of Information Requests

30.1 The Freedom of Information Act covers all recorded information held by the Trust. It is not limited to official documents and it covers, for example, drafts, emails, notes and CCTV recordings. Nor is it limited to information that has been created, so it also covers, for example, letters received from members of the public, although there may be a good reason not to release them.

30.2 Outsourced services undertaken by an external company may hold information on the Trust's behalf. Some of the information held by the external company may be covered by the Act if a freedom of information request is received. The company does not have to answer any requests for information it receives, but they may forward

requests to the Trust.

30.3 The Freedom of Information Act does not cover information the Trust holds solely on behalf of another person, body or organisation. This means employees' purely private information is not covered, even if it is on a work computer or email account; nor is information stored solely on behalf of a trade union, or an individual Governor or Trustee.

30.4 The Freedom of Information Act 2000 provides public access to information held by public authorities. The Act does not give people access to their own personal data (information about themselves) such as their health records or credit reference file. If a member of the public wants to see information that the Trust holds about them, a subject access request under the General Data protection Regulations should be made

30.5 The Trust recognises its duty to:

a. Provide advice and assistance to anyone requesting information. The Trust will respond to straightforward verbal requests for information, and will help enquirers to put more complex verbal requests into writing so that they can be handled under the Act;
b. Tell enquirers whether or not the Trust holds the information they are requesting (the duty to confirm or deny), and provide access to the information the Trust holds in accordance with the procedures laid down in Section 4 of the Compliance Lead's Guide for Management of Information.

30.6 Managing Information Requests

a. The Executive Director of People, Strategy & IT is responsible for responding to information requests that relate to the Trust as a whole, rather than to a specific School. They are also responsible for overseeing the application of this policy, co-ordinating enquiries, leading on any FOI complaints or requests to review decisions and is the lead for any advice, guidance or training.
b. Each school is responsible for responding to information requests that relate to their school, in accordance with the Scheme of Delegation, however this has been limited to responding to the initial requests, any complaints or requests to review decisions have not been delegated, therefore should be referred to the Head of Corporate Governance and Compliance. Each school within the Trust must appoint a Compliance Lead who is responsible for SAR & FOI information requests, this person must be notified to the Executive Director of People, Strategy & IT and join the termly network meeting with the Trust.
c. Schools are required to update the DPO platform 'Jedu' with the information requests that are received, to enable the Trust to have a complete overview and report on all SAR and FOI requests at Trust level.
d. Requests under SAR and FOI can be addressed to anyone in the Trust so all staff will be made aware of the process for dealing with requests and to forward to the Compliance Lead.
e. The Trust has contracted Judicium to provide a platform for each school to register their information requests and a URL link has been created for each school to assist members of the public when submitting requests for information. This URL must be published on each school website.
f. The DPO Judicium will respond to any requests for guidance, enable a request to be directed to the correct place or for a complaint or request for review to be referred. The Executive Director of People, Strategy & IT is responsible for management oversight of the DPO service.
g. The types of request and the subsequent procedure is outlined in Section 4 of the Compliance Lead Guide on the Management of Information.
h. There is a **time limit of 20 school days excluding school holidays** for responding to a request and must be responded to in accordance to the procedures laid down Section 4 of the Compliance Lead Guide on the Management of Information.
i. Certain information is subject to either absolute or qualified exemptions. The exemptions are listed in Section 4.3 of the Compliance Lead Guide for Management of Information. When applying a qualified exemption to a request, the public interest test procedures need to be invoked to determine if public interest in applying the exemption outweighs the public interest in disclosing the information.
j. Unless it is in the public interest to withhold information, it will be released. The Public Interest Test will be applied before any qualified exemptions are invoked. For information on applying the Public Interest Test as noted in Section 4 of the Compliance Lead Guide on the Management of Information.

30.7 Right to refuse

a. The Trust reserves the right to refuse to supply information where the time or cost of doing so exceeds the statutory maximum, currently 18 hours. Members of staff should refer to Section 4 of the Compliance Lead Guide for further information.

32. Training

31.1 All staff and governors are provided with data protection training as part of their induction process.

31.2 Data protection will also form part of continuing professional development, where changes to legislation, guidance or the school's processes make it necessary.

33. Monitoring arrangements

32.1 The DPO is responsible for monitoring and reviewing this policy.

32.2 This policy will be reviewed annually and approved by delegated authority to the Senior Executive team.

32.3 The Trust will instruct the DPO to undertake annual audits to monitor compliance with this policy and the UK GDPR processes, to ensure that all guidance and support is kept up to date and to ascertain where further guidance and support is needed.

34. Transparency and Privacy Notices

33.1 Trust wide privacy notices tailored to the different stakeholder groups/individuals are published on the Trust website and located here.

33.2 When personal data is collected indirectly (for example, from a third party or a publicly available source), where appropriate, we will provide the data subject with the above information as soon as possible after receiving the data. The Trust or school will also confirm whether that third party has collected and processed data in accordance with the UK GDPR.

33.3 Notifications shall be in accordance with ICO guidance and where relevant, be written in a form understandable by those defined as "children" under the UK GDPR.

35. Privacy by Design

34.1 The Trust adopts a privacy by design approach to data protection to ensure that we adhere to data compliance and to implement technical and organisational measures in an effective manner.

34.2 Privacy by design is an approach that promotes privacy and data protection compliance from the start. To help us achieve this, the Trust and its schools take into account the nature and purposes of the processing, any cost of implementation and any risks to rights and freedoms of data subjects when implementing data processes.

36. Complaints

35.1 If a member of the public is unhappy with the service they have received in relation to their request and wish to make a complaint or request a review of the decision, they should be informed to put it in writing to the following contact details, this information should be provided in the letter sent out in response to the request:

Head of Corporate Governance & Compliance,
Head Office: Cranbrook Education Campus,
Tillhouse Road
Exeter EX5 7EE,

dataprotection@tedwraggtrust.co.uk

35.2 The Trust will aim to investigate all complaints within **10 days of receipt**. The complaint will be dealt with by the Head of Corporate Governance & Compliance, or the Director of People, if the Head of Corporate Governance & Compliance dealt with the original information request.

35.3 If on investigation the original decision is upheld, then the Trust has a duty to inform the complainant of their right to appeal to the Information Commissioner's office, which will be detailed in the response letter. Appeals should be made in writing to the Information Commissioner's office at:

FOI/EIR Complaints Resolution
Information Commissioner's Office
Wycliffe House
Water Lane
Wilmslow
Cheshire SK9 5AF

37. Other policies linked

- Privacy Notices
- Computer/Mobile Device Use and Online Policy - Students
- Photographic & Digital Images Policy
- Safeguarding and Child Protection Policy (published on each individual school's website)
- HR Policies including Grievance, Disciplinary and Capability (published on Staff Hub)

38. Further guidance can be found on the Trust's website or in the Management of Information Guide published on the Staff Hub

Trust website

A. How to request information: Freedom of Information (FOI) and Publication Scheme
B. How to request information: Subject Access Request (SAR)
C. Retention Schedule
D. Biometric data in schools
E. CCTV in schools

Compliance Lead Guide on the Management of Information procedures

- Section 2: Personal Data Breaches
- Section 3: Subject Access Requests
- Section 4: Freedom of Information Requests
- Section 4: Public Interest Test
- Section 4: Exemptions
- Section 4: Charging
- Section 5: Data Protection Impact Assessments
- Section 6: Data Processing
- Section 7: Records Management
- Section 8: Retention