Data Protection Policy

Review Summary

Adopted:	**March 2017**
Review Cycle:	**Annual**
Last Review:	**May 2020**
Next Review:	**May 2021**

1. Introduction

1.1. This Policy sets out the obligations of the Trust data regarding data protection and peoples' rights in respect of their personal data under the General Data Protection Regulation ("GDPR").

1.2. 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.

1.3. This Policy sets out the procedures that are to be followed when dealing with personal data. 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.

1.4. The Trust is committed not only to the letter of the law, but also to the spirit of the law and places high importance on the correct, lawful, and fair handling of all personal data, respecting the legal rights, privacy, and trust of all individuals with whom it deals.

1.5. The Information Commissioners Office (ICO) can investigate complaints, audit the Trust's use or other Processing of Personal Data and can take action against the Trust (and individually in some cases) for breach of these laws. Action may include making the Trust pay a fine and/or stopping the use by the Trust of the Personal Data, which may prevent the Trust from carrying on its educational and associated functions. Organisations who breach one or more laws on Personal Data also often receive negative publicity for the breaches which affects the reputation of the Trust and its activities as a result.

1.6. Any breach of or failure to comply with this policy, particularly any deliberate release of Personal Data to an unauthorised third party, may result in disciplinary or other appropriate action.

2. The Data Protection Principles

This Policy aims to ensure compliance with GDPR. GDPR sets out the following principles with which any party handling personal data must comply. All personal data must be:

a. processed lawfully, fairly, and in a transparent manner in relation to the data subject;

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

c. adequate, relevant and limited to what is necessary in relation to the

purposes for which it is processed;

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

e. kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data is 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 GDPR in order to safeguard the rights and freedoms of the data subject;

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

3. Lawful, Fair, and Transparent Data Processing

GDPR seeks to ensure that personal data is processed lawfully, fairly, and transparently, without adversely affecting the rights of the person. 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.

4. 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 GDPR). The purposes for which we process personal data will be informed to data subjects through the publication of Privacy Notices.

5. 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 4, above.

6. 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.

7. 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. 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.

9. Accountability

a. The Trust's Director of Finance & Resources holds accountability for Data Protection through an outsourced Data Protection Officer (DPO) service.

b. 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.

10. Privacy Impact Assessments

The Trust shall carry out Privacy Impact Assessments when and as required under GDPR. Privacy Impact Assessments shall be overseen by the Trust's data protection officer 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 GDPR.

11. The Rights of Data Subjects

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.

12. Keeping Data Subjects Informed – Privacy Notices

The Trust shall ensure that the following information is provided through the publication and sharing of Privacy Notices. The Trust utilise the DfE's Model Privacy Notices and are published on the Trust and Trust schools' websites.

13. Data Subject Access

13.1 A person may make a subject access request ("SAR") at any time to find out more about the personal data which the Trust holds about them. The Trust is normally required to respond to SARs within one month of receipt (this can be extended by up to two months in the case of complex and/or numerous requests, and in such cases the data subject shall be informed of the need for the extension).

13.2 All subject access requests received must be forwarded to the Headteacher of the school it relates to, who will obtain advice from the Trust's data protection officer or directly to the data protection officer for Trust Central Services.

13.3 The Trust does not charge a fee for the 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.

14 Rectification of Personal Data

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).

15 Erasure of Personal Data

15.1 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**.**

15.2 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).

16 Restriction of Personal Data Processing

16.1 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.

17 Data Portability

17.1 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 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).

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

17.3 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).

18 Objections to Personal Data Processing

18.1 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.

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

18.3 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 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.

19 Automated Decision-Making

19.1 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 to such decisions under GDPR, requesting human intervention, expressing their own point of view, and obtaining an explanation of the decision from the Trust.

19.2 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.

20 Profiling

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.

21 Data Protection Measures

21.1 The Trust shall ensure compliance with the following when working with personal data:

a. Laptops, Pads and Data sticks must be encrypted;

b. Digital equipment must be disposed of securely;

c. Paper information that contains sensitive and personal data must be disposed of using a shredder or confidential waste bags;

d. A clear desk policy must be in operation and personal data must be securely locked away when not in use;

e. All hardcopies of personal data, along with any electronic copies stored on physical, removable media should be stored securely in a locked box, drawer, cabinet or similar;

f. Screens must be positioned appropriately so that personal data cannot be seen by the public and the screen is locked when left unattended.

g. All emails sent to external third parties outside the Trust network must be sent using encryption software - 'Egress Switch'.

h. Personal data attached to emails to be avoided where possible. Where it is feasible a link to where the personal data is stored is to be used.

i. Where Personal data is to be transferred in hardcopy form it should be passed directly to the recipient or sent using Special Delivery Mail.

j. Personal data must be handled with care at all times and should not be left unattended or on view to unauthorised employees, agents, sub-contractors or other parties at any time;

k. No personal data should be stored on any mobile device (including, but not limited to, laptops, tablets and smartphones), whether such device belongs to the Trust or otherwise.

l. No personal data should be stored on the computer's hard drive. It must be stored on the Trust network where the data is securely stored and encrypted;

m. All passwords used to protect personal data should not use words or phrases that can be easily guessed or otherwise compromised. All passwords must contain a combination of uppercase and lowercase letters, numbers, and symbols. All software used by the Trust is designed to require such passwords;

n. Under no circumstances should any passwords be written down or shared between any employees, agents, contractors, or other parties working on behalf of the Trust, irrespective of seniority or department. If a password is forgotten, it must be reset using the applicable method. IT staff do not have

access to passwords;

21.2 The Trust will undertake audits to ensure compliance with this policy and the GDPR to ensure that all guidance and support is kept up to date and to ascertain where further guidance and support is needed.

22 Organisational Measures

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 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.

23 Data Breach Notification

23.1 All personal data breaches must be reported immediately to the Headteacher or directly to the Trust's data protection officer in respect of central services.

23.2 If a personal data breach occurs and that breach is likely to result in a risk to the rights and freedoms of data subjects (e.g. financial loss, breach of confidentiality, discrimination, reputational damage, or other significant social or economic damage), the data protection officer must ensure that the Information Commissioner's Office is informed of the breach without delay, and in any event, within 72 hours after having become aware of it.

23.3 In the event that a personal data breach is likely to result in a high risk to the rights and freedoms of data subjects, the data protection officer must ensure that all affected data subjects are informed of the breach directly and without undue delay.

23.4 The data protection officer will undertake the following steps as part of an investigation:

a. Containment and Recovery

- The investigation will determine the appropriate course of action and the required resources needed to limit the impact of the incident. This might require isolating a compromised section of the network, alerting relevant staff or shutting down critical equipment.
- Appropriate steps will be taken to recover system or data losses and resume normal business operation. This might entail attempting to recover any lost equipment, using backup mechanisms to restore compromised or stolen data and changing compromised passwords.
- Advice from experts within and outside the Trust may be sought in resolving the incident promptly and appropriately.

b. Notification

- A decision based on the seriousness of the breach will determine subsequent actions.
- The data protection officer will make a decision to inform any external organisation, such as the police or other appropriate regulatory body.
- If a breach involving Personal Data has occurred, the data protection officer will risk assess whether the Information Commissioner's Office (ICO) needs to be informed, if necessary, based on the extent of the breach.
- Individuals whose Personal Data have been affected by the incident will be notified to enable them to take steps to protect themselves, and where users of Trust information assets have been affected, users will be notified. The notice will include a description of the breach and the steps taken to mitigate the risks.

c. Review

- Once the incident is contained, a thorough review of the event will be undertaken. See Appendix A Data Breach Report Template. The report will detail the root cause of the incident and contributory factors, the chronology of events, response actions, recommendations and lessons learned to identify areas that require improvement.
- Recommended changes to systems, policies and procedures will be documented and implemented as soon as possible thereafter.
- The report will be signed off by the data protection officer and submitted to the Trust Audit Finance and Recourses Committee.

24 Complaints

Complaints will be dealt with in line with the Trust's complaints policy. Please be aware that complaints can be made to the ICO where information relating to Personal Data is concerned.

25 Policy Circulation

25.1 This Policy will be published on the Trust's website, circulated to every staff member as part of the induction process and is included within the staff handbook.

25.2 The Trustees are responsible for overseeing, reviewing and organising the revision of this Policy.

Adoption of the Policy

This Policy has been adopted by the Trustees of the Ted Wragg Multi Academy Trust**.**

Signed

(Chair of Trust)

Date: 04.06.20

Appendix A

PERSONAL DATA SECURITY BREACH REPORT

Time and Date breach was identified	
School	
Description of the Breach	
Name of Person Reporting it:	
Confirmed or suspected Breach	
Volume of Data Involved	
Breach contained or ongoing	
What actions were undertaken to recover the data	
Any other relevant information	

Investigation Checklist

A. Containment and Recovery

Determine severity of breach and if any Personal Data is involved	
Allocate Lead Investigation Officer	
Identify cause of the breach and whether it has been contained. Ensure that any possibility of further data loss is removed or mitigated as far as possible	
Determine whether anything can be done to recover any losses and limit any damage that may be caused E.g. physical recovery of data/equipment, or where data corrupted, through use of back-ups.	
Where appropriate, the Lead Responsible Officer or nominee to inform the police. E.g. stolen property, fraudulent activity, offence under Computer Misuse Act	

B. Assessment of Risks

Type and volume of data How many individuals' Personal Data are affected by breach?	
How sensitive is the data	
What happened to it	
If the data was lost/stolen, were there any protections in place to prevent access/misuse? E.g. encryption of data/device.	
Who are the individuals whose data has been compromised? Students, applicants, staff, customers, clients or suppliers?	
Is there actual/potential harm that could come to any individuals? E.g. are there risks to: • physical safety; • emotional wellbeing; • reputation; • finances; • identify (theft/fraud from release of non-public identifiers); • or a combination of these and other private aspects of their life?	
Are there others who might advise on risks/courses of action? E.g. If individuals' bank details have been lost, consider contacting the banks themselves for advice on anything they can do to help you prevent fraudulent use.	

C. Consideration of Further Notification

Can notification help the Trust meet its security obligations under the seventh data protection principle?	

E.g. prevent any unauthorised access, use or damage to the information or loss of it.	
Can notification help the individual? Could individuals act on the information provided to mitigate risks (e.g. by changing a password or monitoring their account)?	
Consider the dangers of 'over notifying'. Not every incident will warrant notification "and notifying a whole 2 million strong customer base of an issue affecting only 2,000 customers may well cause disproportionate enquiries and work".	
Consult the ICO guidance on when and how to notify it about breaches. Where there is little risk that individuals would suffer significant detriment, there is no need to report. There should be a presumption to report to the ICO where a Approved by RMSG 18 January 2016 large volume of Personal Data is concerned and there is a real risk of individuals suffering some harm. Cases must be considered on their own merits and there is no precise rule as to what constitutes a large volume of Personal Data.	
Consider, as necessary, the need to notify any third parties who can assist in helping or mitigating the impact on individuals. E.g. police, insurers, professional bodies, funders, trade unions, website/system owners, bank/credit card companies.	

D. Evaluation and Response

Establish where any present or future risks lie.	
Consider and identify any weak points in existing security measures and procedures. E.g. in relation to methods of storage and/or transmission, use of storage devices, levels of access, systems/network protections.	
Consider and identify any weak points in levels of security awareness/training.	
Report to LGB and Trust Audit & Resources Committee	

Report Form completed by	
Date	