The Tutor Trust Data Protection Policy

Statement of intent

The Tutor Trust is required to keep and process certain information about its staff members, contractors (including tutors), consultants (including trustees), partners, tutees and other third parties in accordance with its legal obligations under the EU General Data Protection Regulation (GDPR 2018).

The Tutor Trust may, from time to time, be required to share personal information about its staff or pupils with regulatory and potentially children's services.

This policy is in place to ensure all staff and trustees are aware of their responsibilities and outlines how The Tutor Trust complies with the following core principles of the General Data Protection Regulation (GDPR) and Data Protection Act 2018.

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

1. GDPR Definitions:

1.1. Data Controller

Like the existing Data Protection Act 2018 (DPA), the GDPR applies to Data Controllers who process personal data. Data controllers are organisations who decides the purpose for which any personal data is to be processed and the way in which it is to be processed.

1.2. Data Processor

These are organisations that process data on behalf of the Data Controller.

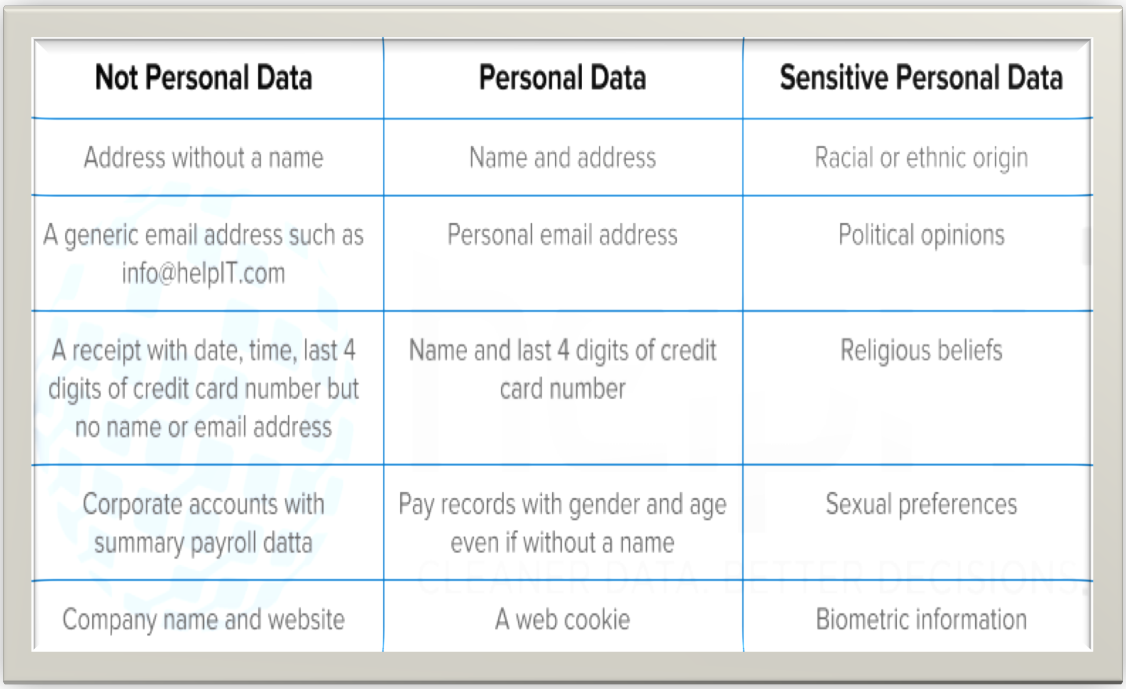
1.3. Personal Data

Personal data is any information relating to an identified or identifiable natural person; i.e. data that identifies a living individua. Each person to which the personal data refers is known as a **Data Subject**.

1.4. Sensitive Personal Data

This includes the following personal data revealing: racial or ethnic origin; political opinions; religious or philosophical beliefs; trade union membership; the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person; an individual's health; a natural person's sex life or sexual orientation; criminal convictions or offences.

The table below illustrates what is sensitive and what isn't, and what isn't personal data:



Not Personal Data	Personal Data	Sensitive Personal Data
Address without a name	Name and address	Racial or ethnic origin
A generic email address such as info@helpIT.com	Personal email address	Political opinions
A receipt with date, time, last 4 digits of credit card number but no name or email address	Name and last 4 digits of credit card number	Religious beliefs
Corporate accounts with summary payroll datta	Pay records with gender and age even if without a name	Sexual preferences
Company name and website	A web cookie	Biometric information

2. Legal framework

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

The General Data Protection Regulation (GDPR), The Freedom of Information Act 2000, The Education (Pupil Information) (England) Regulations 2005 (as amended in 2016), The Freedom of Information and Data Protection (Appropriate Limit and Fees) Regulations 2004

2.2. This policy will be implemented in conjunction with the following Tutor Trust policies/documents:

The Tutor Trust Handbook, The Tutor Trust Safeguarding Policy, The Tutor Trust Privacy Notices, School data sharing agreement, The Tutor Trust Data Inventory.

3. Sources

For the purposes of The Tutor Trust's business, personal or sensitive information may derive from various sources, such as:

- Employees (and close relations, e.g. emergency and next of kin contacts).
- Ex-employees.
- Potential and prospective employees.
- Referees.
- Client records.
- Targeted school individuals (marketing).

- School pupils.
- Trustees/patrons.
- Grant funders/donors/professional partners.
- Tutors.
- Tutor alumni.

4. Principles

4.1. Tutor Trust complies with the data protection principles set out below. In accordance with the requirements outlined in the GDPR, personal data will be:

- Processed lawfully, fairly and in a transparent manner in relation to individuals.
- Collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall not be considered to be incompatible with the initial purposes.
- Adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed.
- Accurate and, where necessary, kept up-to-date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay.
- Kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods, insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes, subject to implementation of the appropriate technical and organisational measures required by the GDPR in order to safeguard the rights and freedoms of individuals.
- Processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.

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

5. Accountability

5.1. The Tutor Trust will demonstrate accountability by implementing policies and procedures, technical and organisational measures and keeping documentation such as breach records and DSAR records.

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

5.3. Records of activities relating to higher risk processing will be maintained, such as the processing of special categories data or that in relation to criminal convictions and offences.

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

- Data minimisation.
- Pseudonymising.
- Anonymising

- Transparency.
- Allowing individuals to monitor processing.
- Continuously creating and improving security features.

5.5. Data protection impact assessments (DPIA) are used, where appropriate.

6. Data protection officer (DPO)

6.1. The DPO has been appointed by trustees in order to:

- Inform and advise The Tutor Trust and its employees about their obligations to comply with the GDPR and other data protection laws.
- Monitor the Tutor Trust's compliance with the GDPR and other laws, including managing internal data protection activities, advising on data protection impact assessments, conducting internal audits and providing the required training to staff members.

6.2. Tutor Trust has appointed Bulletproof (external accredited Data Protection experts) to the role of DPO.

6.3. Bulletproof have professional experience and knowledge of data protection law and will be responsible for overseeing a company's data protection strategy and its implementation to ensure compliance with GDPR requirements.

6.4. The DPO (Bulletproof) will report and liaise with the COO, ICO and board of trustees in data protection matters.

6.5. The DPO will operate independently in performing their DPO duties.

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

7. Lawful processing

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

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

- The consent of the data subject has been obtained.
- Processing is necessary for: Compliance with a legal obligation, the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller, for the performance of a contract with the data subject or to take steps to enter into a contract, protecting the vital interests of a data subject or another person, for the purposes of legitimate interests pursued by the controller or a third party, except where such interests are overridden by the interests, rights or freedoms of the data subject. (This condition is not available to processing undertaken by The Tutor Trust in the performance of its tasks.)

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

- Explicit consent of the data subject
- Processing carried out by a not-for-profit body with a political, philosophical, religious or trade union aim provided the processing relates only to members or former members (or those who have regular contact with it in connection with those purposes) and provided there is no disclosure to a third party without consent.

- Processing relates to personal data manifestly made public by the data subject.
- Processing is necessary for: — Carrying out obligations under employment, social security or social protection law, or a collective agreement protecting the vital interests of a data subject or another individual where the data subject is physically or legally incapable of giving consent, the establishment, exercise or defence of legal claims or where courts are acting in their judicial capacity, reasons of substantial public interest on the basis of Union or Member State law which is proportionate to the aim pursued and which contains appropriate safeguards, the purposes of preventative or occupational medicine, for assessing the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment or management of health or social care systems and services on the basis of Union or Member State law or a contract with a health professional, reasons of public interest in the area of public health, such as protecting against serious cross-border threats to health or ensuring high standards of healthcare and of medicinal products or medical devices, archiving purposes in the public interest, or scientific and historical research purposes or statistical purposes in accordance with Article 89(1).

8. Consent

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

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

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

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

8.5. Consent can be withdrawn by the individual at any time.

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

8.7. Legitimate Interests

The Tutor Trust relies on the legitimate interest basis for some of their uses of constituents' personal data, like performing analytics. Using legitimate interest requires that we:

- Conduct a balancing test.
- Tell constituents that you're relying on legitimate interests;
- Allow constituents to opt out of the processing.

9. PECR

The Tutor Trust complies with both GDPR and the UK's Privacy and Electronic Communication Regulations ("PECR").

Under PECR, to send direct marketing to 'natural persons', The Tutor Trust:

- Will obtain consent where necessary, or
- Marketing to an existing customer in the context of the sale of a product or service. This is referred to as the "soft opt-in." The Tutor Trust sells services so they can take advantage of the 'soft option' only with the appropriate initial consent.

10. Data Subject Rights

Tutor Trust has processes in place to ensure that it can facilitate any request made by an individual to exercise their rights under data protection law. All staff have received training and are aware of the rights of data subjects. Staff can identify such a request and know who to send it to. Refer here to find the Data Subject Rights Request Procedure.

All requests will be considered without undue delay and satisfied within one calendar month of receipt as far as possible.

Tutor Trust will ensure the rights as detailed below can be exercised by data subjects

Informed: The right to be informed about the collection and use of personal data is addressed via company privacy notices.

Subject access: the right to request information about how personal data is being processed, including whether personal data is being processed and the right to be allowed access to that data and to be provided with a copy of that data along with the right to obtain the following information:

- the purpose of the processing
- the categories of personal data
- the recipients to whom data have been disclosed or which will be disclosed
- the retention period
- the right to lodge a complaint with the Information Commissioner's Office
- the source of the information if not collected direct from the subject, and
- the existence of any automated decision-making.

Rectification: the right to allow a data subject to rectify inaccurate personal data concerning them.

Erasure: the right to have data erased and to have confirmation of erasure, but only where:

- the data is no longer necessary in relation to the purpose for which it was collected, or
- where consent is withdrawn, or
- where there is no legal basis for the processing, or
- there is a legal obligation to delete data.

Restriction of processing: the right to ask for certain processing to be restricted in the following circumstances:

- if the accuracy of the personal data is being contested, or
- if our processing is unlawful but the data subject does not want it erased, or
- if the data is no longer needed for the purpose of the processing but it is required by the data subject for the establishment, exercise or defence of legal claims, or
- if the data subject has objected to the processing, pending verification of that objection.

Data portability: the right to receive a copy of personal data which has been provided by the data subject and which is processed by automated means in a format which will allow the individual to transfer the data to another data controller. This would only apply if Tutor Trust was processing the data using consent or based on a contract.

Object to processing: the right to object to the processing of personal data relying on the legitimate interests processing condition unless Tutor Trust can demonstrate compelling legitimate grounds for the processing which override the interests of the data subject or for the establishment, exercise or defence of legal claims.

Object to automated profiling: the right to object where solely automated decision-making is being carried out that has legal or similarly significant effects on the data subject.

11. Data breaches

11.1. The term 'personal data breach' refers to a breach of security which has led to the destruction, loss, alteration, unauthorised disclosure of, or access to, personal data.

11.2. The DPO and COO will ensure that all staff members are made aware of, and understand, what constitutes a data breach as part of their CPD training.

11.3. Where a breach is likely to result in a risk to the rights and freedoms of individuals, the relevant supervisory authority (ICO) will be informed.

11.4. All notifiable breaches will be reported to the trustee responsible for Data Protection and the relevant supervisory authority within 72 hours of The Tutor Trust becoming aware of it.

11.5. The risk of the breach having a detrimental effect on the individual, and the need to notify the relevant supervisory authority, will be assessed on a case-by-case basis.

11.6. In the event that a breach is likely to result in a high risk to the rights and freedoms of an individual, The Tutor Trust will notify those concerned directly.

11.7. A 'high risk' breach means that the threshold for notifying the individual is higher than that for notifying the relevant supervisory authority.

11.8. In the event that a breach is sufficiently serious, the public will be notified without undue delay.

11.9. Effective and robust breach detection, investigation and internal reporting procedures are in place at The Tutor Trust, which facilitate decision-making in relation to whether the relevant supervisory authority or the public need to be notified.

11.10. Within a breach notification, the following information will be outlined:

- The nature of the personal data breach, including the categories and approximate number of individuals and records concerned.
- The name and contact details of the DPO.
- An explanation of the likely consequences of the personal data breach.
- A description of the proposed measures to be taken to deal with the personal data breach.
- Where appropriate, a description of the measures taken to mitigate any possible adverse effects

11.11. Failure to report a breach when required to do so may result in a fine, as well as a fine for the breach itself.

12. Data security

12.1. Confidential paper records will be kept in a locked filing cabinet, drawer or safe, with restricted access.

12.2. Confidential paper records will not be left unattended or in clear view anywhere with general access.

12.3. Digital data is coded, encrypted or password-protected, both on a local hard drive and on a network drive that is regularly backed up off-site.

12.4. Where data is saved on removable storage or a portable device, the device will be kept in a locked filing cabinet, drawer or safe when not in use.

12.5. Memory sticks will not be used to hold personal information unless they are password-protected and fully encrypted.

12.6. All electronic devices are Encrypted and password-protected to protect the information on the device in case of theft.

12.7. Where possible, The Tutor Trust enables electronic devices to allow the remote blocking or deletion of data in case of theft.

12.8. Staff will not use their personal laptops or computers for Tutor Trust purposes.

12.9. All necessary members of staff are provided with their own secure login and password, and every computer regularly prompts users to change their password.

12.10. Emails containing sensitive or confidential information are password protected if there are unsecure servers between the sender and the recipient.

12.11. Circular emails to Tutor Trust stakeholders are sent blind carbon copy (bcc), so email addresses are not disclosed to other recipients.

12.12. Where personal information that could be considered private or confidential is taken off the premises, either in electronic or paper format, staff will take extra care to follow the same procedures for security, e.g. keeping devices under lock and key. The person taking the information from The Tutor Trust premises accepts full responsibility for the security of the data.

12.13. Before sharing data, all staff members will ensure:

- They are allowed to share it.

- That adequate security is in place to protect it.
- Who will receive the data has been outlined in a privacy notice.

12.14. Under no circumstances are visitors allowed access to confidential or personal information. Visitors to areas of The Tutor Trust containing sensitive information are supervised at all times.

12.15. The physical security of the Tutor Trust's buildings and storage systems, and access to them, is reviewed on a yearly basis. If an increased risk in vandalism/burglary/theft is identified, extra measures to secure data storage will be put in place.

12.16. The Tutor Trust takes its duties under the GDPR seriously and any unauthorised disclosure may result in disciplinary action.

12.17. The DPO and COO are responsible for continuity and recovery measures that are in place to ensure the security of protected data.

13. Data Transfers

Tutor Trust will ensure that any personal data transferred to third countries or third parties in third countries will not be transferred without suitable safeguards which may include:

- Standard contract clauses with published ICO Addendum
- International data transfer agreement as published by the ICO
- Adequacy decision
- An exception as defined in Article 49 of the GDPR

14. Publication of information

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

- Policies and procedures.
- Annual reports.

14.2. Classes of information specified in the publication scheme are made available quickly and easily on request.

14.3. The Tutor Trust will not publish any personal information, including photos, on its website without the permission of the affected individual.

14.4. When uploading information to the Tutor Trust website, staff are considerate of any metadata or deletions which could be accessed in documents and images on the site.

15. Videos and photography

15.1. The Tutor Trust understands that recording images of identifiable individuals constitutes as processing personal information, so it is done in line with data protection principles.

15.2. The Tutor Trust will always indicate its intentions for taking photographs of pupils and tutors and will retrieve permission before publishing them.

15.3. If The Tutor Trust wishes to use images/video footage of pupils in a publication, such as The Tutor Trust website or Impact Report, written permission will be sought for the particular usage from the parent of the pupil (through the school.)

16. Data retention

16.1. Data will not be kept for longer than is necessary and in-line with relevant legislation. All data retained will be reviewed annually.

16.2. Unrequired data will be deleted as soon as practicable.

16.3. Some records relating to employees of The Tutor Trust may be kept for an extended period for legal reasons, but also to enable the provision of references.

16.4. Paper documents will be shredded or pulped, and electronic memories scrubbed clean or destroyed, once the data should no longer be retained.

17. DBS data

17.1. All data provided by the DBS will be handled in line with data protection legislation; this includes electronic communication.

17.2. Data provided by the DBS will never be duplicated.

17.3. Any third parties who access DBS information will be made aware of the data protection legislation, as well as their responsibilities as a data handler.

18. The Tutor Trust Employees' Responsibility

18.1. Compliance with this Policy is the responsibility of every employee of The Tutor Trust (including temporary employees and consultants), and any person who acts on behalf of The Tutor Trust and any person who has responsibilities for the collection, access or processing of personal data.

18.2. Employees must understand what is meant by personal and sensitive data, and know how to handle such data.

18.3. Each employee of The Tutor Trust is required to:-

- Read and understand this Data Protection Policy.
- Complete and pass compulsory GDPR online training and read updates as directed.
- Adhere and abide to this Data Protection Policy.
- Share best practices on data protection issues.
- Read and adhere to any changes or updates to this Data Protection Policy when notified of such changes or updates.
- Report concerns relating to data protection to The Tutor Trust's COO.

19. Contractors, Data Processors, Consultants, Agents and other Third Parties

19.1. All contractors, Data Processors, agents, consultants, partners, sub-contractors and other third parties acting on behalf of The Tutor Trust, including tutors, must:

- Ensure that they and all employees who have access to personal data held or processed for or on behalf of The Tutor Trust, are aware of this policy and are fully aware of their duties and responsibilities under the GDPR
- Any breach of any provision of GDPR will be deemed as being a breach of any contract between The Tutor Trust and that individual, company, partner, organisation or firm
- Allow data protection audits by The Tutor Trust of personal data held on its behalf (if requested)
- Indemnify The Tutor Trust against any prosecution, claims proceedings, actions or payments of compensation or damages, without limitation.

19.2. All contractors, Data Processors, agents, consultants, partners, sub-contractors and other third parties who are users of personal data supplied by The Tutor Trust must confirm they have a compliant data protection register entry in the ICO's public register, and must provide security guarantees at least equivalent to the technical and organisational measures The Tutor Trust has adopted to ensure compliance the GDPR Act.

20. Clear Desk Policy

The Tutor Trust operates a clear desk policy in the office. Employees must follow the guidelines below:

- All personal information should be locked away when desks are unattended, especially overnight. Particularly sensitive information may need to be kept in a fire-retardant cabinet or safe.
- Where the volume of paperwork prevents it from being locked away, it should still be kept tidy and out of the way as far as possible. Files, boxes and crates blocking corridors or fire exits create a safety hazard.
- All papers should be collected immediately from printers and faxes.
- Particular care should be taken of documents taken outside the office.
- GDPR data protection regulations apply to data about individuals which is created, stored, transmitted or disclosed as a paper record.
- Computers should be locked if desks are left unattended for any period of time. Further, a full log out should be completed prior to leaving the office.

21. The Tutor Trust trustees' responsibility

21.1. Tutor Trust Trustees are responsible for data protection and are charged with ensuring that Tutor Trust officers operate in compliance with this policy. The board of trustees have overall responsibility for ensuring the Tutor Trust compliance with data protection legislation covering the UK and the European Economic Community. The DPO (Bulletproof) and COO are responsible for providing guidance, training, updates and advice on the Policy.

21.2. A review will be completed on an annual basis to provide reasonable assurance that the policy and procedures are working effectively and to enable risk areas to be identified and addressed.

22. Policy review

22.1. This policy is reviewed annually by the DPO (Bulletproof and COO) and approved by the trustees.

22.2. The next scheduled review date for this policy is April 2024.

For further information please contact:

Data Protection Officer
Units H/J/K Arlington Business Park Gateway 1000, Whittle Way, Stevenage, Herts, SG1 2FP.
T: 0143 853 2915 | DDI: 014 385 32915 | E: DPOSupport@bulletproof.co.uk

The Tutor Trust - Chief Operating Officer who is the GDPR Lead within the organisation.
Tel: 0161 833 3055
Email: privacy@thetutortrust.org