Data Protection Policy

1. INTRODUCTION

1.1. Qualified Tutor collects and uses certain types of personal information about staff, pupils, parents and other individuals who come into contact with the organisation in order provide education and associated functions. Qualified Tutor may be required by law to collect and use certain types of information to comply with statutory obligations related to employment, education and safeguarding and this policy is intended to ensure that personal information is dealt with properly and securely and in accordance with the General Data Protection Regulation ("GDPR") and other related legislation.

1.2. The GDPR applies to all computerised data and manual files if they come within the definition of a filing system. Broadly speaking, a filing system is one where the data is structured in some way that it is searchable on the basis of specific criteria (so you would be able to use something like the individual's name to find their information), and if this is the case, it does not matter whether the information is located in a different physical location.

1.3. This policy will be updated as necessary to reflect best practice or amendments made to data protection legislation and shall be reviewed every [2] years.

2. PERSONAL DATA

2.1. 'Personal data' is information that identifies an individual and includes information that would identify an individual to the person to whom it is disclosed because of any special knowledge that they have or can obtain[1]. A sub-set of personal data is known as 'special category personal data'. This special category data is information that relates to:

2.1.1. race or ethnic origin;

2.1.2. political opinions;

2.1.3.religious or philosophical beliefs;

2.1.4.trade union membership;

2.1.5.physical or mental health;

2.1.6.an individual's sex life or sexual orientation;

2.1.7.genetic or biometric data for the purpose of uniquely identifying a natural person.

2.2. Special Category information is given special protection and additional safeguards apply if this information is to be collected and used.

2.3. Information relating to criminal convictions shall only be held and processed where there is legal authority to do so.

2.4 The organisation does not intend to seek or hold sensitive personal data about staff or participants except where the organisation has been notified of the information, or it comes to the organisation's attention via legitimate means (e.g. a sign up) or needs to be sought and held in compliance with a legal obligation or as a matter of good practice. Staff or participants are under no obligation to disclose to the organisation their race or ethnic origin, political or religious beliefs, whether or not they are a trade union member or details of their sexual life (save to the extent that details of marital status and/or parenthood are needed for other purposes, e.g. pension entitlements). Where information about ethnic group is processed, this will be used for the purposes of equality monitoring only, as permitted by the Data Protection Act 2018, and will not be used to make any decisions about the individual.

3. THE DATA PROTECTION PRINCIPLES

3.1. The six data protection principles as laid down in the GDPR are followed at all times:

3.1.1.personal data shall be processed fairly, lawfully and in a transparent manner, and processing shall not be lawful unless one of the processing conditions can be met;

3.1.2.personal data shall be collected for specific, explicit, and legitimate purposes, and shall not be further processed in a manner incompatible with those purposes;

3.1.3.personal data shall be adequate, relevant, and limited to what is necessary for the purpose(s) for which it is being processed;

3.1.4. personal data shall be accurate and, where necessary, kept up to date;

3.1.5. personal data processed for any purpose(s) shall not be kept for longer than is necessary for that purpose/those purposes;

3.1.6. personal data shall be processed in such a way that ensures appropriate security of the data, including protection against unauthorised or unlawful processing and against accidental loss, destruction, or damage, using appropriate technical or organisational measures (using a data processing agreement where appropriate).

3.2. In addition to this, the organisation is committed to ensuring that at all times, anyone dealing with personal data shall be mindful of the individual's rights under the law (as explained in more detail in paragraphs 7 and 8 below).

3.3. The organisation is committed to complying with the principles in 3.1 at all times. This means that the organisation will:

3.3.1. inform individuals as to the purpose of collecting any information from them, as and when we ask for it;

3.3.2. be responsible for checking the quality and accuracy of the information;

3.3.3. regularly review the records held to ensure that information is not held longer than is necessary, and that it has been held in accordance with the records retention policy;

3.3.4. ensure that when information is authorised for disposal it is done appropriately;

3.3.5. ensure appropriate security measures to safeguard personal information whether it is held in paper files or on our computer system, and follow the relevant security policy requirements at all times;

3.3.6. share personal information with others only when it is necessary and legally appropriate to do so and keep accurate records (using a data sharing agreement where appropriate);

3.3.7. set out clear procedures for responding to requests for access to personal information known as subject access requests;

3.3.8. report any breaches of the GDPR in accordance with the procedure in paragraph 9 below.

4. CONDITIONS FOR PROCESSING IN THE FIRST DATA PROTECTION PRINCIPLE

4.1. The individual has given consent that is specific to the particular type of processing activity and that consent is informed, unambiguous and freely given.

4.2. The processing is necessary for the performance of a contract to which the individual is a party or is necessary for the purpose of taking steps with regard to entering into a contract with the individual, at their request.

4.3. The processing is necessary for the performance of a legal obligation to which we are subject.

4.4. The processing is necessary to protect the vital interests of the individual or another.

4.5. The processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested on us.

4.6. The processing is necessary for a legitimate interest of the organisation or that of a third party, except where this interest is overridden by the rights and freedoms of the individual concerned.

5. USE OF PERSONAL DATA BY THE ORGANISATION

5.1. The organisation holds personal data on staff, participants, other individuals and anyone who sign up or joins the community. In each case, the personal data must be treated in accordance with the data protection principles as outlined in paragraph 3.1 above.

Staff

5.2 The personal data held about staff will include contact details, employment history, information relating to career progression, information relating to DBS and other pre-employment checks and photographs.

5.3. The data is used to comply with legal obligations placed on the organisation in relation to employment. The organisation may pass information to other regulatory authorities where appropriate and may use names and photographs of staff in publicity and promotional material. Personal data will also be used when giving references.

5.4 Staff should note that information about disciplinary action may be kept for longer than the duration of the sanction. Although treated as “spent” once the period of the sanction has expired, the details of the incident may need to be kept for a longer period.

5.5. Any wish to limit or object to the uses to which personal data is to be put should be notified to the Data Protection Lead who will ensure that this is recorded, and adhered to if appropriate. If the Data Protection Lead is of the view that it is not appropriate to limit the use of personal data in the way specified, the individual will be given written reasons why the organisation cannot comply with their request.

Other Individuals

5.6 The organisation may hold personal information in relation to other individuals who have contact with the organisation, such as volunteers and guests. Such information shall be held only in accordance with the data protection principles and shall not be kept longer than necessary.

6. SECURITY OF PERSONAL DATA

6.1. The organisation will take reasonable steps to ensure that members of staff will only have access to personal data where it is necessary for them to carry out their duties. All staff will be made aware of this Policy and their duties under the GDPR. The organisation will take all reasonable steps to ensure that all personal information is held securely and is not accessible to unauthorised persons.

6.2. For further details with regard to security of IT systems, please refer to the ICT Policy.

7. DISCLOSURE OF PERSONAL DATA TO THIRD PARTIES

7.1. The following list includes the most usual reasons that the organisation will authorise disclosure of personal data to a third party:

7.1.1. To give a confidential reference relating to a current or former employee, volunteer or participant

7.1.2. for the prevention or detection of crime;

7.1.3. for the assessment of any tax or duty;

7.1.4. where it is necessary to exercise a right or obligation conferred or imposed by law upon the organisation (other than an obligation imposed by contract);

7.1.5. for the purpose of or in connection with legal proceedings (including prospective legal proceedings);

7.1.6. for the purpose of obtaining legal advice;

7.1.7. for research, historical and statistical purposes (so long as this neither supports decisions in relation to individuals, nor causes substantial damage or distress);

7.1.8. to disclose details of a pupil's medical condition where it is in the pupil's interests to do so, for example for medical advice, insurance purposes;

7.1.9 to provide information to the relevant Government Department concerned with national education. At the time of the writing of this Policy, the Government Department concerned with national education is the Department for Education (DfE). The Examination Authority may also pass information to the DfE.

7.2 The organisation may receive requests from third parties (i.e. those other than the data subject, the organisation, and employees of the organisation) to disclose personal data it holds about staff or other individuals. This information will not generally be disclosed unless one of the specific exemptions under data protection legislation which allow disclosure applies; or where necessary for the legitimate interests of the organisation or the third party to which the information will be disclosed (except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject).

7.3 All requests for the disclosure of personal data must be sent to the Data Protection Lead, who will review and decide whether to make the disclosure, ensuring that reasonable steps are taken to verify the identity of that third party before making any disclosure.

8. OTHER RIGHTS OF INDIVIDUALS

8.1. The organisation has an obligation to comply with the rights of individuals under the law, and takes these rights seriously. The following section sets out how the organisation will comply with the rights to:

8.1.1. object to processing;

8.1.2. rectification;

8.1.3. erasure; and

8.1.4. data portability.

Right to object to processing

8.2. An individual has the right to object to the processing of their personal data on the grounds of pursuit of a public interest or legitimate interest (grounds 4.5 and 4.6 above) where they do not believe that those grounds are made out.

8.3. Where such an objection is made, it must be sent to the Data Protection Lead within 2 working days of receipt, and the Data Protection Lead will assess whether there are compelling legitimate grounds to continue processing which override the interests, rights and freedoms of the individuals, or whether the information is required for the establishment, exercise or defence of legal proceedings.

8.4. The Data Protection Lead shall be responsible for notifying the individual of the outcome of their assessment within [10] of working days of receipt of the objection.

Right to rectification

8.5. An individual has the right to request the rectification of inaccurate data without undue delay. Where any request for rectification is received, it should be sent to the Data Protection Lead within 2 working days of receipt and where adequate proof of inaccuracy is given, the data shall be amended as soon as reasonably practicable, and the individual notified.

8.6. Where there is a dispute as to the accuracy of the data, the request and reasons for refusal shall be noted alongside the data, and communicated to the individual. The individual shall be given the option of a review under the data protection complaints procedure, or an appeal direct to the Information Commissioner.

8.7. An individual also has a right to have incomplete information completed by providing the missing data, and any information submitted in this way shall be updated without undue delay.

Right to erasure

8.8. Individuals have a right, in certain circumstances, to have data permanently erased without undue delay. This right arises in the following circumstances:

8.8.1. where the personal data is no longer necessary for the purpose or purposes for which it was collected and processed;

8.8.2. where consent is withdrawn and there is no other legal basis for the processing;

8.8.3. where an objection has been raised under the right to object, and found to be legitimate;

8.8.4. where personal data is being unlawfully processed (usually where one of the conditions for processing cannot be met);

8.8.5. where there is a legal obligation on the organisation to delete.

8.9. The Data Protection Lead will make a decision regarding any application for erasure of personal data and will balance the request against the exemptions provided for in the law. Where a decision is made to erase the data and this data has been passed to other data controllers and/or has been made public, reasonable attempts to inform those controllers of the request shall be made.

Right to restrict processing

8.10. In the following circumstances, processing of an individual's personal data may be restricted:

8.10.1. where the accuracy of data has been contested, during the period when the organisation is attempting to verify the accuracy of the data;

8.10.2. where processing has been found to be unlawful and the individual has asked that there be a restriction on processing rather than erasure;

8.10.3. where data would normally be deleted, but the individual has requested that their information be kept for the purpose of the establishment, exercise or defence of a legal claim;

8.10.4. where there has been an objection made under paragraph 11.2 above, pending the outcome of any decision.

Right to portability

8.11. If an individual wants to send their personal data to another organisation they have a right to request that the organisation provides their information in a structured, commonly used and machine readable format. As this right is limited to situations where the organisation is processing the information on the basis of consent or performance of a contract, the situations in which this right can be exercised will be quite limited. If a

request for this is made, it should be forwarded to the Data Protection Lead within 2 working days of receipt, and the Data Protection Lead will review and revert as necessary.

9 . BREACH OF ANY REQUIREMENT OF THE GDPR

9.1 Any and all breaches of the GDPR, including a breach of any of the data protection principles shall be reported as soon as it is discovered, to the Data Protection Lead.

9.2 Once notified, the Data Protection Lead shall assess:

9.2.1 the extent of the breach;

9.2.2 the risks to the data subject(s) as a consequence of the breach;

9.2.3 any security measures in place that will protect the information;

9.2.4 any measures that can be taken immediately to mitigate the risk to the individual(s).

9.3 Unless the Data Protection Lead concludes that there is unlikely to be any risk to individuals from the breach, it must be notified to the Information Commissioner's Office within 72 hours of the breach having come to the attention of the organisation, unless a delay can be justified.

9.4 The Information Commissioner shall be told:

9.4.1 details of the breach, including the volume of data at risk and the number and categories of data subjects;

9.4.2 the contact point for any enquiries (which shall usually be the Data Protection Lead);

9.4.3 the likely consequences of the breach;

9.4.4 measures proposed or already taken to address the breach.

9.5 If the breach is likely to result in a high risk to the rights and freedoms of the affected individuals, then the Data Protection Lead shall notify data subjects of the breach without undue delay unless the data would be unintelligible to those not authorised to access it or measures have been taken to mitigate any risk to the affected individuals.

9.6 Data subjects shall be told:

9.6.1 the nature of the breach;

9.6.2 who to contact with any questions;

9.6.3 measures taken to mitigate any risks.

9.7 The Data Protection Lead shall then be responsible for instigating an investigation into the breach, including how it happened and whether it could have been prevented. Any recommendations for further training or a change in procedure shall be reviewed by the Governing Body and a decision made about implementation of those recommendations.

10 . CONTACT

10.1 If anyone has any concerns or questions in relation to this Policy they should contact the Data Protection Lead.

This policy was approved by the Qualified Tutor Company Founder Julia Silver

November 2023
Review Frequency: ANNUAL

---

[1] For example, if asked for the number of female employees, and you only have one female employee, this would be personal data if it was possible to obtain a list of employees from the website/organisation.