

# DATA PROTECTION POLICY (UK GDPR) (Employees/Workers/Contractors)

## 1 Overview

- 1.1 The Trust takes the security and privacy of your data seriously. We need to gather and use information or 'data' about you as part of our business and to manage our relationship with you. We intend to comply with our legal obligations under the **Data Protection Act 2018** (the '2018 Act') and the UK **General Data Protection Regulation** ('UK GDPR') in respect of data privacy and security. We have a duty to notify you of the information contained in this policy.
- 1.2 This policy applies to current and former employees, workers, volunteers, apprentices, members, trustees, governors and consultants. If you fall into one of these categories then you are a 'data subject' for the purposes of this policy. You should read this policy alongside your contract of employment (or contract for services) and any other notice we issue to you from time to time in relation to your data. This policy is in place to ensure all staff and governors are aware of their responsibilities and outlines how the Trust complies with the 2018 Act and UK GDPR.
- 1.3 The Trust has separate policies and privacy notices in place in respect of pupils and parents. A copy of these can be obtained on the Trust's website.
- 1.4 The Trust has measures in place to protect the security of your data. The Trust will hold data in accordance with our Data Retention Policy. A copy of this can be obtained from HR. We will only hold data for as long as necessary for the purposes for which we collected it.
- 1.5 The Trust is a '**data controller**' for the purposes of your personal data. This means that we determine the purpose and means of the processing of your personal data.
- 1.6 This policy explains how the Trust will hold and process your information. It explains your rights as a data subject. It also explains your obligations when obtaining, handling, processing or storing personal data in the course of working for, or on behalf of, the Trust.

- 1.7 Your compliance with this Data Protection Policy is mandatory. Related policies and privacy notices are available to help you interpret and act in accordance with this Data Protection Policy. You must also comply with all such related policies and privacy guidelines.
- 1.8 This policy does not form part of your contract of employment (or contract for services if relevant) and can be amended by the Trust at any time. It is intended that this policy is fully compliant with the 2018 Act and the UK GDPR. If any conflict arises between those laws and this policy, the Trust intends to comply with the 2018 Act and the UK GDPR.
- 1.9 The Trust's Data Protection Officer ('DPO') is Euan Imrie ([dpo@cltrust.co.uk](mailto:dpo@cltrust.co.uk)). The DPO is responsible for overseeing this Data Protection Policy and, as applicable, developing related policies and privacy guidelines.

## 2 Data Protection Principles

- 2.1 Personal data must be processed in accordance with six '**Data Protection Principles**.' It must:
- be processed fairly, lawfully and transparently;
  - be collected and processed only for specified, explicit and legitimate purposes;
  - be adequate, relevant and limited to what is necessary for the purposes for which it is processed;
  - be accurate and where necessary kept up to date. Any inaccurate data must be deleted or rectified without delay;
  - not be kept for longer than is necessary for the purposes for which it is processed;
  - be processed securely using appropriate technical and organisational measures to protect against authorised or unlawful processing and accidental loss, destruction or damage;
  - not be transferred to another country without appropriate safeguards being in place; and
  - be made available to data subjects and allow data subjects to exercise certain rights in relation to their personal data.

We are accountable for these principles and must be able to show that we are compliant.

## 3 How we define personal data

- 3.1 '**Personal data**' means information which relates to a living person who can be **identified** from that data (a '**data subject**') on its own, or when taken together with other information which is likely to come into our possession. It includes any expression of opinion about the person and an indication of the intentions of us or others, in respect of that person. It does not include anonymised data.

3.2 This policy applies to all personal data whether it is stored electronically, on paper or on other materials.

3.3 This personal data might be provided to us by you, or someone else (such as a former employer, your doctor, or a credit reference agency), or it could be created by us. It could be provided or created during the recruitment process or during the course of the contract of employment (or services) or after its termination. It could be created by your manager or other colleagues.

3.4 We will collect and use the following types of personal data about you:

- recruitment information such as your application form and CV, references, qualifications and membership of any professional bodies and details of any pre-employment assessments;
- your contact details and date of birth;
- the contact details for your emergency contacts;
- your gender;
- your marital status and family details;
- information about your contract of employment (or services) including start and end dates of employment, role and location, working hours, details of promotion, salary (including details of previous remuneration), pension, benefits and holiday entitlement;
- your bank details and information in relation to your tax status including your national insurance number;
- your identification documents including passport and driving licence and information in relation to your immigration status and right to work for us;
- information relating to disciplinary or grievance investigations and proceedings involving you (whether or not you were the main subject of those proceedings);
- information relating to your performance and behaviour at work;
- training records;
- electronic information in relation to your use of IT systems/swipe cards/telephone systems;
- your images (whether captured on CCTV, by photograph or video);
- qualifications and subjects taught; and
- any other category of personal data which we may notify you of from time to time.

#### **4 How we define special categories of personal data**

4.1 **'Special categories of personal data'** are types of personal data consisting of information as to:

- your racial or ethnic origin;
- your political opinions;
- your religious or philosophical beliefs;
- your trade union membership;
- your genetic or biometric data;
- your health;

- your sex life and sexual orientation; and
- any criminal convictions and offences.

We may hold and use any of these special categories of your personal data in accordance with the law.

## **5 How we define processing**

5.1 **'Processing'** means any operation which is performed on personal data such as:

- collection, recording, organisation, structuring or storage;
- adaption or alteration;
- retrieval, consultation or use;
- disclosure by transmission, dissemination or otherwise making available;
- alignment or combination;
- restriction, destruction or erasure; and
- transmitting or transferring to third parties.

This includes processing personal data which forms part of a filing system and any automated processing.

## **6 How will we process your personal data?**

6.1 The Trust will process your personal data (including special categories of personal data) in accordance with our obligations under the 2018 Act.

6.2 We will use your personal data:

- to perform the contract of employment (or services) between us;
- to comply with any legal obligation;
- where it is in the public interest;
- where we need to protect your interests, or someone else's interests (such as a pupil); or
- if it is necessary for our legitimate interests (or for the legitimate interests of someone else). However, we can only do this if your interests and rights do not override ours (or theirs). You have the right to challenge our legitimate interests and request that we stop this processing. See details of your rights in section 12 below.

We can process your personal data for these purposes without your knowledge or consent. We will not use your personal data for an unrelated purpose without telling you about it and the legal basis that we intend to rely on for processing it.

If you choose not to provide us with certain personal data you should be aware that we may not be able to carry out certain parts of the contract between us. For example, if you do not provide us with your bank account details we may not be able to pay you. It might also stop us from complying with certain legal obligations and duties which we

have such as to pay the right amount of tax to HMRC or to make reasonable adjustments in relation to any disability you may suffer from.

## **7 Examples of when we might process your personal data**

7.1 We have to process your personal data in various situations during your recruitment, employment (or engagement) and even following termination of your employment (or engagement).

7.2 For example (and see section 7.5 below for the meaning of the asterisks):

- to decide whether to employ (or engage) you;
- to decide how much to pay you, and the other terms of your contract with us;
- to check you have the legal right to work for us;
- to carry out the contract between us including where relevant, its termination;
- training you and reviewing your performance\*;
- to decide whether to promote you;
- to decide whether and how to manage your performance, absence or conduct\*;
- to carry out a disciplinary or grievance investigation or procedure in relation to you or someone else;
- to determine whether we need to make reasonable adjustments to your workplace or role because of your disability\*;
- to monitor diversity and equal opportunities\*;
- to monitor and protect the security (including network security) of the Trust, of you, our other staff, pupils and others;
- to monitor and protect the health, safety and welfare of you, our other staff, pupils and third parties\*;
- to pay you and provide pension and other benefits in accordance with the contract between us\*;
- paying tax and national insurance;
- to provide a reference upon request from another employer;
- to pay trade union subscriptions\*;
- monitoring compliance by you, us and others with our policies and our contractual obligations\*;
- to comply with employment law, immigration law, health and safety law, tax law and other laws which affect us\*;
- to answer questions from insurers in respect of any insurance policies which relate to you\*;
- running the Trust and planning for the future;
- the prevention and detection of fraud or other criminal offences;
- to defend the Trust in respect of any investigation or litigation and to comply with any court or tribunal orders for disclosure\*;
- to safeguard pupils;
- for any other reason which we may notify you of from time to time.

7.3 We will only process special categories of your personal data (see above) in certain situations in accordance with the law. For example, we can do so if we have your explicit consent. If we asked for your consent to process a special category of personal data then we would explain the reasons for our request. You do not need to consent and can withdraw consent later if you choose.

7.4 We do not need your consent to process special categories of your personal data when we are processing it for the following purposes, which we may do:

- where it is necessary for carrying out rights and obligations under employment law;
- where it is necessary to protect your vital interests or those of another person; where you/they are physically or legally incapable of giving consent;
- where you have made the data public;
- where processing is necessary for the establishment, exercise or defence of legal claims; and
- where processing is necessary for the purposes of occupational medicine or for the assessment of your working capacity.

7.5 We might process special categories of your personal data for the purposes in paragraph 7.2 above which have an asterisk beside them. In particular, we will use information in relation to:

- your race or ethnic origin to monitor equal opportunities;
- your sickness absence, health and medical conditions to monitor your absence, assess your fitness for work, to pay you benefits, to comply with our legal obligations under employment law including to make reasonable adjustments and to look after your health and safety; and
- your trade union membership to pay any subscriptions and to comply with our legal obligations in respect of trade union members.

7.6 We envisage that we will hold information about criminal convictions as it is appropriate given the nature of the role you work in, and to comply with our legal obligations. Where appropriate, we will collect information about criminal convictions as part of the recruitment process or we may be notified of such information directly by you in the course of you working for us. We will use information about criminal convictions and offences in order to maintain appropriate safeguards for working with children.

7.7 We do not take automated decisions about you using your personal data or use profiling in relation to you.

## **8 Sharing your personal data**

8.1 Sometimes we might share your personal data with other schools in the Trust or our contractors and agents to carry out our obligations under our contract with you or for our legitimate interests. Further details of such third parties is set out in the Privacy Notice.

- 8.2 We require those companies to keep your personal data confidential and secure and to protect it in accordance with the law and our policies. They are only permitted to process your data for the lawful purpose for which it has been shared and in accordance with our instructions.
- 8.3 We do not send your personal data outside the European Economic Area. If this changes you will be notified of this and the protections which are in place to protect the security of your data will be explained.

## **9 How should you process personal data for the Trust?**

- 9.1 Everyone who works for, or on behalf of, the Trust has some responsibility for ensuring data is collected, stored and handled appropriately.
- 9.2 The Trust's DPO is responsible for reviewing this policy and updating the Board of Trustees on the Trust's data protection responsibilities and any risks in relation to the processing of data. You should direct any questions in relation to this policy or data protection to this person.
- 9.3 You should only access personal data covered by this policy if you need it for the work you do for, or on behalf of the Trust and only if you are authorised to do so. You should only use the data for the specified lawful purpose for which it was obtained.
- 9.4 You should not share personal data informally.
- 9.5 You should keep personal data secure and not share it with unauthorised people.
- 9.6 You should regularly review and update personal data which you have to deal with for work. This includes telling us if your own contact details change.
- 9.7 You should not make unnecessary copies of personal data and should keep and dispose of any copies securely.
- 9.8 You should use strong passwords.
- 9.9 You should lock your computer screens when not at your desk.
- 9.10 You should ensure that individual monitors do not show confidential information to passers-by.
- 9.11 Personal data should be encrypted where particularly sensitive before being transferred electronically to authorised external contacts. Speak to IT for more information on how to do this.
- 9.12 Consider anonymising data or using separate keys/codes so that the data subject cannot be identified.

- 9.13 Except in limited circumstances and where necessary, do not save personal data to your own personal computers or other devices.
- 9.14 Personal data should never be transferred outside the European Economic Area except in compliance with the law and authorisation of the DPO.
- 9.15 You should lock drawers and filing cabinets, where possible. Do not leave paper with personal data lying about.
- 9.16 You should not take personal data away from Trust's premises without authorisation from your line manager or DPO.
- 9.17 You must maintain data security by protecting the confidentiality, integrity and availability of personal data defined as follows:
- Confidentiality means that only people who have a need to know and are authorised to use the personal data can access it,
  - Integrity means that personal data is accurate and suitable for the purpose for which it is processed.
  - Availability means that authorised users are able to access the personal data when they need it for authorised purposes.
- 9.18 Personal data should be shredded and disposed of securely when you have finished with it.
- 9.19 You should ask for help from our DPO (or the DPO's nominated representative in each school) if you are unsure about data protection or if you notice any areas of data protection or security we can improve upon.
- 9.20 Any deliberate or negligent breach of this policy by you may result in disciplinary action being taken against you in accordance with our disciplinary procedure.
- 9.21 It is a criminal offence to conceal or destroy personal data which is part of a subject access request (see below). This conduct would also amount to gross misconduct under our disciplinary procedure, which could result in your dismissal.

## **10 How to deal with data breaches**

- 10.1 We have robust measures in place to minimise and prevent data breaches from taking place. Should a breach of personal data occur (whether in respect of you or someone else) then we must take notes and keep evidence of that breach. If the breach is likely to result in a risk to the rights and freedoms of individuals then we must also notify the Information Commissioner's Office within 72 hours.
- 10.2 If you are aware of a data breach you must contact the DPO immediately and keep any evidence you have in relation to the breach.

10.3 Please see the Trust's Personal Data Breach Procedure for further details.

## **11 Subject access requests**

11.1 Data subjects can make a '**subject access request**' ('SAR') to find out the information we hold about them. This request must be made in writing. If you receive such a request you should forward it immediately to the DPO who will coordinate a response.

11.2 If you would like to make a SAR in relation to your own personal data you should make this in writing to the DPO. We must respond within one month unless the request is complex or numerous in which case the period in which we must respond can be extended by a further two months. The individual will be informed of this extension, and will receive an explanation of why the extension is necessary, within one month of the receipt of the request. The Trust will verify the identity of the person making the request before any information is supplied.

11.3 There is no fee for making a SAR. However, if your request is manifestly unfounded, excessive or a request for further copies of the same information we may charge a reasonable administrative fee or refuse to respond to your request. The individual will be informed of a decision to refuse to respond to the request and the reasoning behind it, as well as their right to complain to the supervisory authority and to a judicial remedy, within one month of the refusal.

11.4 In the event that a large quantity of information is being processed about an individual, the Trust will ask the individual to specify the information the request is in relation to.

## **12 Your data subject rights**

12.1 You have the right to information about what personal data we process, how and on what basis as set out in this policy. The following rights are provided to you:

- the right to be informed;
- the right of access;
- the right to rectification;
- the right to erasure;
- the right to restrict processing;
- the right to data portability;
- the right to objection
- rights in relation to automated decision making and profiling.

12.2 You have the right to access your own personal data by way of a subject access request (see above).

12.3 The right to rectification:

- You can correct any inaccuracies in your personal data. To do so, you should contact HR.
- Where the personal data in question has been disclosed to third parties, the Trust will inform them of the rectification where possible. Where appropriate, the Trust will inform the individual about the third parties that the data has been disclosed to.
- Requests for rectification will be responded to within one month; this will be extended by two months where the request for rectification is complex.
- Where no action is being taken in response to a request for rectification, the Trust will explain the reason for this to the individual, and will inform them of their right to complain to the supervisory authority and to a judicial remedy.

#### 12.4 The right to erasure:

- You have the right to request that we erase your personal data where we were not entitled under the law to process it or it is no longer necessary to process it for the purpose it was collected. To do so you should contact HR.
- The Trust has the right to refuse a request for erasure where the personal data is being processed for the following reasons:
  - To exercise the right of freedom of expression and information
  - To comply with a legal obligation for the performance of a public interest task or exercise of official authority
  - For public health purposes in the public interest
  - For archiving purposes in the public interest, scientific research, historical research or statistical purposes
  - The exercise or defence of legal claims
- Where personal data has been disclosed to third parties, they will be informed about the erasure of the personal data, unless it is impossible or involves disproportionate effort to do so.
- Where personal data has been made public within an online environment, the Trust will inform other organisations who process the personal data to erase links to and copies of the personal data in question

#### 12.5 The right to restriction:

- While you are requesting that your personal data is corrected or erased or are contesting the lawfulness of our processing, you can apply for its use to be restricted while the application is made. To do so you should contact HR.
- In the event that processing is restricted, the Trust will store the personal data, but not further process it, guaranteeing that just enough information about the individual has been retained to ensure that the restriction is respected in future.
- The Trust will restrict the processing of personal data where the Trust no longer needs the personal data but the individual requires the data to establish, exercise or defend a legal claim.

- If the personal data in question has been disclosed to third parties, the Trust will inform them about the restriction on the processing of the personal data, unless it is impossible or involves disproportionate effort to do so.
- The Trust will inform individuals when a restriction on processing has been lifted.

#### 12.6 The right to object:

- You have the right to object to data processing where we are relying on a legitimate interest to do so and you think that your rights and interests outweigh our own and you wish us to stop. Where personal data is processed for the performance of a legal task or legitimate interests, an individual's grounds for objecting must relate to his or her particular situation. The Trust will stop processing the individual's personal data unless the processing is for the establishment, exercise or defence of legal claims, or, where the Trust can demonstrate compelling legitimate grounds for the processing, which override the interests, rights and freedoms of the individual.
- You have the right to object if we process your personal data for the purposes of direct marketing. The Trust will stop processing personal data for direct marketing purposes as soon as an objection is received. The Trust cannot refuse an individual's objection regarding data that is being processed for direct marketing purposes.

#### 12.7 The right to data portability:

- You have the right to receive a copy of your personal data and to transfer your personal data to another data controller in relation to:
  - personal data that an individual has provided to a controller;
  - processing based on the individual's consent or for the performance of a contract;
  - processing carried out by automated means.
- We will not charge for this and will in most cases aim to do this within one month. Where the request is complex, or a number of requests have been received, the timeframe can be extended by two months, ensuring that the individual is informed of the extension and the reasoning behind it within one month of the receipt of the request.
- Where no action is being taken in response to a request, the Trust will, without delay and at the latest within one month, explain to the individual the reason for this and will inform them of their right to complain to the supervisory authority and to a judicial remedy.
- Personal data will be provided in a structured, commonly used and machine-readable form but the Trust is not required to adopt or maintain processing systems which are technically compatible with other organisations.
- Where feasible, data will be transmitted directly to another organisation at the request of the individual.

- In the event that the personal data concerns more than one individual, the Trust will consider whether providing the information would prejudice the rights of any other individual.

12.8 With some exceptions, you have the right not to be subjected to automated decision-making.

12.9 You have the right to be notified of a data security breach concerning your personal data.

12.10 In most situations we will not rely on your consent as a lawful ground to process your data. If we do however request your consent to the processing of your personal data for a specific purpose, you have the right not to consent or to withdraw your consent later. To withdraw your consent, you should contact the DPO.

12.11 You have the right to complain to the Information Commissioner. You can do this by contacting the Information Commissioner's Office directly. Full contact details including a helpline number can be found on the Information Commissioner's Office website ([www.ico.org.uk](http://www.ico.org.uk)). This website has further information on your rights and our obligations.

## **13 Questions**

13.1 Please contact the DPO with any questions about the operation of this Data Protection Policy or the UK GDPR or if you have any concerns that this Data Protection Policy is not being or has not been followed. In particular, you must always contact the DPO in the following circumstances:

- if you are unsure of the lawful basis which you are relying on to process personal data (including the legitimate interests used by the Trust);
- if you are unsure about the retention period for the personal data being processed;
- if you are unsure about what security or other measures you need to implement to protect personal data;
- if there has been a personal data breach;
- if you need any assistance dealing with any rights invoked by a data subject; and
- if you plan to undertake any activities involving automated processing.

## **14 Changes to this policy**

14.1 We reserve the right to change this policy at any time. Where appropriate, we will notify data subjects of those changes by mail or email.