

# Data Protection Policy

## Introduction

Wells Cathedral is committed to being transparent about how it collects and uses the personal data of its workforce, and to meeting its data protection obligations. This policy sets out Wells Cathedral's commitment to data protection, and individual rights and obligations in relation to personal data.

This policy applies to the personal data of job applicants, employees, workers, contractors, volunteers, interns, apprentices, and former employees, referred to as HR-related personal data. Questions about this policy, or requests for further information, should be directed to your Line Manager.

## Definitions

"*Personal data*" is any information that relates to a living individual who can be identified from that information.

"*Processing*" is any use that is made of data, including collecting, storing, amending, disclosing, or destroying it.

"*Special categories of personal data*" means information about an individual's racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, health, sex life or sexual orientation and genetic and biometric data.

"*Criminal records data*" means information about an individual's criminal convictions and offences, and information relating to criminal allegations and proceedings.

## Data Protection Principles

Wells Cathedral processes HR-related personal data in accordance with the following data protection principles:

- Lawfully, fairly and in a transparent manner.
- Wells Cathedral collects personal data only for specified, explicit and legitimate purposes, and only where it is adequate, relevant, and limited to what is necessary for the purposes of processing.
- Wells Cathedral keeps accurate personal data and takes all reasonable steps to ensure that inaccurate personal data is rectified or deleted without delay.
- Wells Cathedral keeps personal data only for the period necessary for processing.
- Wells Cathedral adopts appropriate measures to make sure that personal data is secure, and protected against unauthorised or unlawful processing, and accidental loss, destruction, or damage.

Wells Cathedral tells individuals the reasons for processing their personal data, how it uses such data and the legal basis for processing in its privacy notices. It will not process personal data of individuals for other reasons. If Wells Cathedral wants to start processing HR-related data for other reasons, individuals will be informed of this before any processing begins.

HR-related data will only be shared with the HR Consultant. Where Wells Cathedral relies on its legitimate interests as the basis for processing data, it will carry out an assessment to ensure that those interests are not overridden by the rights and freedoms of individuals.

Where Wells Cathedral processes special categories of personal data or criminal records data to perform obligations, to exercise rights in employment law, or for reasons of substantial public interest, this is done in accordance with the requirements for processing special category data and criminal records data.

Wells Cathedral will update HR-related personal data promptly if an individual advises that their information has changed or is inaccurate.

Personal data gathered during the employment, worker, contractor or volunteer relationship, apprenticeship or internship, is held in the individual's personnel file (in hard copy or electronic format, or both). The periods for which Wells Cathedral holds HR-related personal data are contained in its privacy notices to individuals.

Wells Cathedral keeps a record of its processing activities in respect of HR-related personal data in accordance with the requirements of the UK General Data Protection Regulation (UK GDPR).

## Individual Rights

As a data subject, individuals have several rights in relation to their personal data.

## **Data Subject Access Requests (DSARs)**

Individuals have the right to make a subject access request. If an individual makes a subject access request, Wells Cathedral will tell them:

- Whether or not their data is processed and if so why, the categories of personal data concerned and the source of the data if it is not collected from the individual.
- To whom their data is or may be disclosed, including to recipients located outside the UK and the safeguards that apply to such transfers.
- For how long their personal data is stored (or how that period is decided).
- Their rights to rectification or erasure of data, or to restrict or object to processing.
- Their right to complain to the Information Commissioner if they think Wells Cathedral has failed to comply with their data protection rights; and
- whether or not Wells Cathedral carries out automated decision-making and the logic involved in any such decision-making.

Wells Cathedral will also provide the individual with a copy of the personal data undergoing processing. This will normally be in electronic form if the individual has made a request electronically unless they agree otherwise. To make a subject access request, the individual should send the request to a director. In some cases, proof of identification may be required before the request can be processed. Wells Cathedral will inform the individual if it needs to verify their identity and the documents it requires.

Wells Cathedral will normally respond to a request within a period of one month from the date it is received. In some cases, such as where the request is complex, it may respond within three months of the date the request is received. Wells Cathedral will write to the individual within one month of receiving the original request to tell them if this is the case.

If a subject access request is manifestly unfounded or excessive, Wells Cathedral is not obliged to comply with it. Alternatively, Wells Cathedral can agree to respond but will charge a fee, which will be based on the administrative cost of responding to the request. A subject access request is likely to be manifestly unfounded if it is made with the intention of harassing Wells Cathedral or causing disruption, or excessive where it repeats a request to which Wells Cathedral has already responded. If an individual submits a request that is unfounded or excessive, Wells Cathedral will notify them that this is the case and whether it will respond to it.

## **Other Rights**

Individuals have several other rights in relation to their personal data. They can require Wells Cathedral to:

- Rectify inaccurate data.
- Stop processing or erase data that is no longer necessary for the purposes of processing.
- Stop processing or erase data if the individual's interests override Wells Cathedral's legitimate grounds for processing data (where Wells Cathedral relies on its legitimate interests as a reason for processing data).
- Stop processing or erase data if processing is unlawful; and
- Stop processing data for a period if data is inaccurate or if there is a dispute about whether the individual's interests override Wells Cathedral's legitimate grounds for processing data.

To ask Wells Cathedral to take any of these steps, the individual should send the request to the Chief Operating Officer.

## **Data Security**

Wells Cathedral takes the security of HR-related personal data seriously. Wells Cathedral has internal policies and controls in place to protect personal data against loss, accidental destruction, misuse, or disclosure, and to ensure that data is not accessed, except by employees in the proper performance of their duties.

Where Wells Cathedral engages third parties to process personal data on its behalf, such parties do so based on written instructions, are under a duty of confidentiality and are obliged to implement appropriate technical and organisational measures to ensure the security of data.

## **Data Protection Impact Assessments (DPIAs)**

Some of the processing that Wells Cathedral carries out may result in risks to privacy. Where processing would result in a high risk to individual rights and freedoms, Wells Cathedral will carry out a data protection impact assessment to determine the necessity and proportionality of processing. This will include considering the purposes for which the activity is carried out, the risks for individuals and the measures that can be put in place to mitigate those risks.

## **Data breaches**

If Wells Cathedral discovers that there has been a breach of HR-related personal data that poses a risk to the rights and freedoms of individuals, it will report it to the Information Commissioner within 72 hours of discovery. Wells Cathedral will record all data breaches regardless of their effect.

If the breach is likely to result in a high risk to the rights and freedoms of individuals, it will tell affected individuals that there has been a breach and provide them with information about its likely consequences and the mitigation measures it has taken.

## **International Data Transfers**

Wells Cathedral will not transfer HR-related personal data to countries outside the UK.

## **Individual Responsibilities**

Individuals are responsible for helping Wells Cathedral keep their personal data up to date. Individuals should let Wells Cathedral know if data provided changes, for example if an individual moves house or changes bank details. Individuals may have access to the personal data of other individuals, and of our customers and clients in the course of their employment, contract, volunteer period, internship, or apprenticeship. Where this is the case, Wells Cathedral relies on individuals to help meet its data protection obligations to employees, and to customers and clients.

Individuals who have access to personal data are required:

- Only to access data that they have authority to access and only for authorised purposes.
- Not to disclose data except to individuals (whether inside or outside Wells Cathedral) who have appropriate authorisation.
- To keep data secure (for example by complying with rules on access to premises, computer access, including password protection, and secure file storage and destruction).
- Not to remove personal data, or devices containing or that can be used to access personal data, from Wells Cathedral's premises without adopting appropriate security measures (such as encryption or password protection) to secure the data and the device.
- Not to store personal data on local drives or on personal devices that are used for work purposes; and
- To report data breaches of which they become aware to the Chief Operating Officer or the Financial Controller, or HR Consultant immediately.

Failing to observe these requirements may amount to a disciplinary offence, which will be dealt with under Wells Cathedral's disciplinary procedure. Significant or deliberate breaches of this policy, such as accessing employee or customer data without authorisation or a legitimate reason to do so, may constitute gross misconduct and could lead to dismissal without notice.

## **Training**

Wells Cathedral will provide training to all individuals about their data protection responsibilities as part of the induction process.

Individuals whose roles require regular access to personal data, or who are responsible for implementing this policy or responding to subject access requests under this policy, will receive additional training to help them understand their duties and how to comply with them.

## **Privacy Notice**

Wells Cathedral is a "data controller". This means that we are required under data protection legislation to notify you of how we will process your personal data both during the employment relationship and post termination. This notice will explain how we collect your personal data, its use, storage, transfer, and security. We will also explain what rights you have in relation to how we process your personal data. It is important that you read this notice,

together with any other privacy notice we may provide during your employment, so that you are aware of how and why we are processing your personal data. This notice does not form part of any contract of employment or other contract to provide services. We may update this notice at any time.

### **What are our obligations to you in relation to how we process your personal data?**

We are required by law to ensure that when processing any of your personal data that it is:

- Used lawfully, fairly and in a transparent way.
- Collected only for valid purposes that we have clearly explained to you and not used in any way that is incompatible with those purposes.
- Relevant to the purposes we have told you about and limited only to those purposes.
- Accurate and kept up to date.
- Kept in a form which permits you to be identified for only as long as necessary for the purposes we have told you about.
- Kept securely.

### **What personal data will we collect, use and store about you?**

- Your name, salutation (title?), addresses, contact numbers, and personal email addresses
- Date of birth
- Gender
- Next of kin and emergency contact information
- National Insurance number
- Bank account details, payroll records and tax status information
- Salary, annual leave, pension, and benefits information
- Start date
- Location of employment or workplace
- Copy of driving licence
- Recruitment information (including copies of right to work documentation, reference and other information included in a CV or cover letter or as part of the application process)
- Employment records (including job titles, work history, working hours, training records and professional memberships).
- Compensation history
- Performance information
- Disciplinary and grievance information
- CCTV footage and other information obtained through electronic means such as swipe card records
- Information about your use of our information and communications systems
- Photographs
- We may also collect, store, and use the following “special categories” of more sensitive personal information:
  - Information about your race or ethnicity, religious beliefs, sexual orientation and political opinions.
  - Information about your health, including any medical condition, health and sickness records
  - Genetic information and biometric data.
  - Information about criminal convictions and offences

### **How do we collect your personal data?**

We collect your personal data by a variety of means. At recruitment stage we have already collected data through the application process. We may sometimes collect additional information from third parties including former employers, credit reference agencies.

Whilst you are working with us we may need to collect periodically additional personal information from you not identified on the above list, but before doing so we will provide you with a written notice setting out details of the purpose and the lawful basis of why we are collecting that data, its use, storage and your rights.

### **How will we use your personal data?**

For the most part we will use your personal data for one of the following lawful reasons:

- a) Where we need to perform the contract we have entered into with you.
- b) Where we need to comply with a legal obligation.

- c) Where it is necessary for our legitimate interests (or those of a third party) and your interests and fundamental rights do not override those interests.

There are other rare occasions where we may use your personal data, which are:

- d) Where we need to protect your interests (or someone else's interests).  
e) Where it is needed in the public interest or for official purposes.

### **When will we use your personal data?**

During your employment and for a short period after the relationship has ended, we will use your personal information for specific purposes. The list below describes the purpose of our processing, the personal data involved and the lawful basis for our processing:

- Determining the terms on which you work for us
- Checking your right to work in the UK
- When making payments to you to also include any necessary tax and NI deductions
- Liaising with your pension provider and making payments
- Administration related to the performance of a contract of employment
- Business management and work force planning, including accounting and auditing
- Conducting and managing reviews of performance and determining performance requirements
- Making decisions regarding remuneration, bonus, commission and compensation
- Making decisions regarding promotions to include assessing qualifications for a particular role
- Gathering evidence for a possible disciplinary process or gathering evidence in respect of an informal complaint or grievance
- Making decisions about your continued employment or engagement
- Making arrangements for the termination of our working relationship
- Education, training and development requirements
- Dealing with legal disputes involving you or other employees, workers and contractors, including accidents at work
- Managing sickness absence, ascertaining your fitness to work
- Complying with Health and Safety obligations, completion of accident book and RIDDOR reporting
- Prevention of fraud through CCTV monitoring
- Monitoring use of our information and communication systems to ensure compliance with our internal procedures and prevention of security lapses and breach of data protection laws
- Preventing malicious software distribution
- Gathering data analytics to assess retention and attrition rates
- Equal opportunities monitoring

It is possible that some of the grounds for processing will overlap.

### **Your failure to provide information**

We will only ask you to provide information which we believe is necessary for the performance of the contractual employment relationship (for example bank account details to pay you) or our associated legal obligations (for example giving salary information to HMRC). If you fail to provide certain information when requested, we may not be able to meet our contractual obligations to you or we may not be able to fulfil our legal obligations.

### **What happens if we need to use your personal data for a new purpose?**

We will only use your personal data for the stated purposes, unless we consider that there is a need to use it for another reason and that reason is compatible with the original purpose. However, if we consider that it is necessary and reasonable to use your personal data for an unrelated purpose, we will notify you and explain the legal basis which allows us to do so.

There may be circumstances where we have to process your personal data without your knowledge or consent, where this is required by law and in compliance with the above rules.

### **How do we use your sensitive personal information data?**

Any personal data which reveals your ethnic origin, political opinions, religious and philosophical beliefs, trade union membership, genetic, biometric or health data, sex life and sexual orientation will be regarded as special categories of personal data. We will only use this data in the following ways:

- In order to comply with employment and other laws when processing and managing situations connected with absences arising in relation to your sickness or family/dependent related leave.

- To ensure we meet our Health and Safety obligations towards you and other employment related obligations. We will use information about your physical or mental health or disability status to assess your capability to perform your role, monitor and manage your sickness absence, provide appropriate workplace adjustments, and administer health related benefits.
- Where it is needed in the public interest, for example for equal opportunity monitoring and reporting.

There may be circumstances where we need to process this type of information for legal claims or to protect your interests (or someone else's) and you are not able capable of giving your consent or where the relevant information has already been made public.

### **Do we need your consent to use sensitive personal data?**

If we are using your personal sensitive data in accordance with our written policy to perform our legal obligations or exercise specific rights connected to your employment, we do not need your written consent to use this data.

However, in limited circumstances, we may request your written consent to allow us to process your sensitive personal data. For example, your written consent will be required before we instruct a medical practitioner to prepare a medical report. If it becomes necessary to request your consent to process your sensitive personal data, we will provide you with details of the information that we require and why we need it, so that you can decide whether you wish to provide your consent. It is not a condition of your contract of employment with us that you must agree to any request for consent. Giving consent will always be a decision made by your freewill/choice.

### **Will we share your personal data with third parties?**

In order to meet our legal obligations connected with your employment it is necessary to share your personal information with certain third parties (see below). We also need to share your data when we have legitimate business reasons for doing so and also where it is necessary in order to fulfil your contract.

### **Third party service providers and data security**

Third party service providers are only permitted to process your personal data in accordance with our specified instructions. They are also required to take appropriate measures to protect your privacy and personal information. We do not allow your information to be used by third parties for their own purposes and business activities.

### **How do we ensure your personal data is secure?**

We take your privacy and protection of data very seriously. Consequently, we have put in place appropriate security measures to prevent unauthorised use of your personal data. We will notify you and any applicable regulator of any suspected unauthorised use of your personal data.

### **Your duty to inform us of any changes**

In order that we can ensure that the personal data we hold in relation to you is accurate, it is important that you keep us informed of any changes to that data.

### **What rights do you have in respect of how we use your personal data?**

Subject to legal limitations you have the right to:

- **Request access to your data:** You can ask us to provide a copy of the personal data we hold about you.
- **Request corrections to be made to your data:** If you think that your personal data is incomplete or inaccurate you can ask us to correct it.
- **Request erasure of your data:** If you consider there is no lawful basis for us to continue processing your data you can ask for that data to be deleted or removed.
- **Object to the processing of your data:** If our lawful basis for processing your data relates to a legitimate business interest (or third-party interest) you can raise an objection to that interest. You can also object to us using your information for direct marketing purposes.
- **Request that processing restrictions be put in place:** If you believe that your information is being

processed without a lawful reason or that the information is incorrect you can request that a freeze/restriction is placed on the processing of the information until your concerns are addressed.

- **Request a transfer of your personal data:** You can ask us to transfer your personal data to a third party.
- If you wish to exercise any of the above rights, please contact the Chief Operating Officer..

### **Will I have to pay a fee?**

You will not be expected to pay a fee to obtain your personal data unless we consider that your request for access to data is unfounded or excessive. In these circumstances we may charge you a reasonable fee or refuse to comply with your request.

### **Confirmation of identity**

Whenever you make a request for access to personal data, we may request specific information to confirm your identity. This is usually done to ensure that we are releasing personal data to the correct person.

### **Right to withdraw your consent**

If we have asked for your written consent to obtain information, you have the right to withdraw your consent at any time. To withdraw your consent please contact the Chief Operating Officer. Once we receive your notice of withdrawal, we will cease processing your data unless we have any other lawful basis on which to continue processing that data.

### **Important information about this privacy notice**

We reserve the right to amend or update this privacy notice at any time. We will provide you with a new notice when we make any updates.

### **How to make a complaint**

To exercise all relevant rights, queries or complaints please in the first instance contact the Chief Operating Officer. If this does not resolve your complaint to your satisfaction, you have the right to lodge a complaint with the Information Commissioners Office on 0303 123 1113 or via email <https://ico.org.uk/global/contact-us/email/> or at the Information Commissioner's Office, Wycliffe House, Water Lane, Wilmslow, Cheshire, SK9 5AF, England.