**Data and General Data Protection Regulation (GDPR) Policy**

# Privacy notice for employees/workers

In accordance with the General Data Protection Regulation (EU) 2016/679 (GDPR) and the Data Protection Act 2018, Gwent Wildlife Trust (GWT) have implemented this privacy notice to inform you, our employees, of the types of data we process about you. We also include within this notice the reasons for processing your data, the lawful basis that permits us to process it, how long GWT keep your data for and your rights regarding your data. This notice applies to current and former employees and workers.

Data Protection Principles

“Personal Data” means any information relating to an identified or identifiable living individual who can be identified, directly or indirectly in particular by reference to –

* An identifier such as a name, an identification number, location data or an online identifier
* One or more factors specific to the physical, psychological, genetic, mental, economic, cultural or social identity of the individual

Under GDPR, all personal data obtained and held by us must be processed according to a set of core principles. In accordance with these principles, we will ensure that:

* processing is fair, lawful and transparent
* data is collected for specific, explicit, and legitimate purposes
* data collected is adequate, relevant and limited to what is necessary for the purposes of processing
* data is kept accurate and up to date. Data which is found to be inaccurate will be rectified or erased without delay.
* data is not kept for longer than is necessary for its legal or given purpose
* data is processed in a manner that ensures appropriate security of personal data including protection against unauthorised or unlawful processing, accidental loss, destruction or damage by using appropriate technical or organisation measures
* we comply with the relevant GDPR procedures for international transferring of personal data

Types of Data Held

The organisation collects and processes a range of information about you. GWT keep this data in a personnel file relating to each employee and we also hold the data within our computer systems. This includes (as applicable):

* Information provided by you such as your name, address, contact details, email address, telephone number, date of birth and gender
* Job title, Job description, Salary and the terms and conditions of your employment
* Details of your qualifications, skills, experience, employment history, including start and end dates with previous employers and with the organisation
* Information about your pay and benefits
* Details of your bank account and national insurance number
* Information about your marital status, next of kin, dependants and emergency contacts
* Information about your nationality and entitlement to work in the UK
* Information from references
* Information on DBS checks including the outcome of the checks
* Details of your work pattern (days of work and working hours)
* Building access records
* CCTV footage
* IT Equipment use, including internet access and telephones
* All incoming calls are automatically recorded using our 3CX telephony system, the number, date and conversation are recorded in order to protect the Trust and it’s staff.
* Details of periods of leave taken by you, including holiday, sickness and other absence and the reasons for the leave
* Details of any disciplinary or grievance procedures in which you have been involved, including any warnings issued to you and related correspondence
* Performance management information, including appraisals, performance reviews and ratings, training you have participated in, performance improvement plans and related correspondence
* Information about medical or health conditions, including whether or not you have a disability for which the organisation needs to make reasonable adjustments
* Information on your driving license for insurance purposes on Gwent Wildlife Trust pool vehicles
* Equal opportunities monitoring information, including information about your ethnic origin, sexual orientation, health and religion or belief

Collecting Your Data

GWT collect this information in a variety of ways. For example, data is collected through application forms and CVs; obtained from your passport or other identity documents; from forms completed by you at the start of or during employment; from correspondence with you; or through interviews, meetings or other assessments. In some cases, we collect personal data about you from third parties, such as references supplied by former employers and information from DBS checks permitted by law.

Data is stored in our protected 365 system and backed up daily to our cloud storage facility and can only be accessed by authorised employees plus a personnel file stored in a locked cabinet with restricted access.

Lawful Basis for Processing

The law on data protection allows us to process your data for certain reasons only. In the main, GWT process your data in order to comply with a legal requirement or in order to enter into and effectively manage the employment contract we have with you. In other cases, GWT have a legitimate interest in processing personal data before, during and after the end of the employment relationship. Where we rely on legitimate interests as a reason for processing employee personal data, it has been considered whether or not those interests are overridden by the rights and freedoms of employees and we have concluded that they are not.

Some special categories of personal data such as information about health or medical conditions are processed to carry out employment law obligations. Where GWT process other special categories of personal data, such as information about ethnic origin, sexual orientation, health or religious belief, this is done for the purposes of equal opportunities monitoring. Data collected for this purpose is anonymised or is collected with the express consent of employees, which can be withdrawn at any time. Employees are entirely free to decide whether or not to provide such data and there are no consequences of failing to do so. Records are stored in personnel files and can be amended or deleted if an employee so wishes.

The information below categorises the types of data processing, appropriate to your status, we undertake and the lawful basis we rely on.

|  |  |
| --- | --- |
| **Activity Requiring your data** | **Lawful basis for processing** |
| Carry out the employment contract that we have entered into with you | Performance of Contract |
| Salary Payments | Performance of Contract |
| Payment of Income Tax and National Insurance | Legal Obligation |
| Payment of pension | Legal Obligation |
| Carry out checks on an employee’s entitlement to work in the United Kingdom | Legal Obligation |
| Make reasonable adjustments for disabled employees | Legal Obligation |
| Compliance with health and safety laws | Legal Obligation |
| Criminal Records checks to ensure that individuals are permitted to undertake or continue delivering the role | Legal Obligation |
| Run recruitment processes | Legitimate interests |
| Maintain accurate and up-to-date employment records and contact details, and records of employee contractual and statutory rights | Legitimate interests |
| Operate and keep a record of disciplinary and grievance processes | Legitimate interests |
| Operate and keep a record of employee performance and related processes, to plan for career development, succession planning and workforce management | Legitimate interests |
| Operate and keep a record of absence and absence management procedures, to allow effective workforce management and to ensure that employees are receiving the pay or other benefits to which they are entitled | Legitimate interests |
| Operate and keep a record of other types of leave (including maternity, paternity, adoption, parental, shared parental leave and sabbatical), to allow effective workforce management, to ensure that the organisation complies with duties in relation to leave entitlement, and to ensure that employees are receiving the pay or other benefits to which they are entitled | Legitimate interests |
| Ensure effective general HR and business administration | Legitimate interests |
| Provide references on request for current or former employees | Legitimate interests |
| Respond to and defend against legal claims | Legitimate interests |
| Maintain and promote equality, diversity and inclusion in the workplace | Consent |
| Preventing fraud | Legitimate interests |
| Ensuring our administrative and IT systems are secure and robust against unauthorised access | Legitimate interests |

Special Categories of Data

Special categories of personal data processed by GWT are:

* health
* sexual orientation
* race
* ethnic origin
* political opinion
* religion
* trade union membership

GWT carry out processing activities using special category data:

* for the purposes of equal opportunities monitoring
* for sickness absence management procedures
* to determine reasonable adjustments

Most commonly, GWT will process special categories of data when the following applies:

* you have given explicit consent to the processing
* we must process the data in order to carry out our legal obligations
* we must process data for reasons of substantial public interest
* you have already made the data public.

Failure to Provide Data

Your failure to provide GWT with the following data may mean that we are unable to fulfil our requirements for entering into a contract of employment with you:

* Proof of your right to live and work in the United Kingdom
* National Insurance number
* Tax status and payments within the current tax year
* Driving licence
* Qualifications or certificates of competence
* Medical history
* Criminal conviction data

This could include being unable to offer you employment, or administer contractual benefits.

Criminal Conviction Data

GWT will only collect criminal conviction data where it is appropriate given the nature of your role and where the law permits us. This data will usually be collected at the recruitment stage, however, it may also be collected during your employment. We use criminal conviction data to determine your suitability, or your continued suitability, for the role. We rely on the lawful basis of **our legitimate interests** to process this data.

Who GWT Share Your Data With

Employees within our company who have responsibility for recruitment, administration of payment and contractual benefits and the carrying out of performance related procedures will have access to your data which is relevant to their function. All employees with such responsibility have been trained to ensure data is processed in line with GDPR.

Data is shared with third parties for the following reasons: **for the administration of payroll, pensions and benefits.** We have a data processing agreement in place with such third parties to ensure data is not compromised. Third parties must implement appropriate technical and organisational measures to ensure the security of your data. GWT does not share your data with bodies outside of the European Economic Area.

Protecting Your Data

GWT is aware of the requirement to ensure your data is protected against accidental loss or disclosure, destruction and abuse. We have implemented the following processes to guard against this;

* Staff with access to such data are trained in appropriate processing of personal data.
* GWT store data between an on premises server, which is backed to a cloud system currently operated by Microsoft and all data is stored in UK based servers and cloud storage via Microsoft 365. All systems are password protected and available to staff with the requisite clearance.
* Human Resources information is stored in a secure server which is only accessible by authorised employees and backed up off site daily. Back up facilities are outlined above.
* Paper files are kept in a locked file accessible only by the CEO, Head of Finance, Finance & Administration Officer and HR Manager.

Data Breach Notification

A personal data breach is a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or processed. In the event that GWT becomes aware of a breach, or a potential breach, an investigation will be carried out by the Data Protection Officer who will record all breaches and make the decision to notify the Information Commissioner’s Office and individuals affected by the breach within 72 hours.

* If a data breach occurs it will be investigated within 24 hours of receiving notification wherever possible by the data protection officer.
* Upon completion GWT legally have to report incidents to the ICO if the breach results in risk to the rights and freedoms of an individual\s within 72 hours. If this occurs the individual\s affected will be notified in the same timeframe.

Retention Periods

GWT only keep your data for as long as we need it, which will be at least for the duration of your employment with us, though in some cases we will keep your data for a period after your employment has ended. Some data retention periods are set out in law. Retention periods can vary depending on why we need your data:

* Leavers files are retained for six years after the employee’s leave date. Except where legislation dictates the data has to be retained for longer periods.
* Safeguarding records:
  + Pertaining to a child are stored until the child is 25
  + Pertaining to concerns about an adults’ behaviour around children, will be stored until the adult is 65 or for 10 years after these concerns were raised; whichever is longer
  + Pertaining to concerns about behaviour towards vulnerable adults, will be stored for between three and thirty years depending on the severity of the incident; in line with “Department Of Health Protection of Vulnerable Adults Scheme Record Retention and Disposal Policy 2010”
* Financial information is stored for 7 years
* Health records relating to Asbestos, Hazardous substances, Biological tests, Hand Arm Vibration and Whole Body Vibration (questionnaires and screening) are stored for 40 years
* Telephone calls are stored for 90 days and are then automatically deleted unless part of an internal investigation.

Automated Decision Making

Automated decision making means making decisions about you using no human involvement e.g. using computerised filtering equipment. No decision will be made about you solely on the basis of automated decision making (where a decision is taken about you using an electronic system without human involvement) which has a significant impact on you.

Employee Rights

You have the following rights in relation to the personal data we hold on you:

* the right to be informed about the data we hold on you and what we do with it;
* the right of access to the data we hold on you. More information on this can be found in our separate policy on Subject Access Requests;
* the right for any inaccuracies in the data we hold on you, however they come to light, to be corrected. This is also known as ‘rectification’;
* the right to have data deleted in certain circumstances. This is also known as ‘erasure’;
* the right to restrict the processing of the data;
* the right to transfer the data we hold on you to another party. This is also known as ‘portability’;
* the right to object to the inclusion of any information;
* the right to regulate any automated decision-making and profiling of personal data.

More information can be found on each of these rights below.

The right to be informed

You will not be charged for receiving our privacy notices. Our privacy notices set out:

* the types of data GWT hold and the reason for processing the data;
* our legitimate interest for processing it;
* details of who your data is disclosed to and why, including transfers to other countries; where data is transferred to other counties, the safeguards used to keep your data secure are explained;
* how long we keep your data for, or how we determine how long to keep your data for;
* where your data comes from;
* your rights as a data subject;
* your absolute right to withdraw consent for processing data where consent has been provided and no other lawful reason for processing your data applies;
* your right to make a complaint to the Information Commissioner if you think your rights have been breached;
* whether we use automated decision making and if so how the decisions are made, what this means for you and what could happen as a result of the process;
* the name and contact details of our data protection officer.

The right of access

You have the right to access your personal data which is held by us, subject access requests may be made verbally but we would advise that you make a subject access request in writing. Requests should be made using the subject access request form (Appendix 2), the request should be accompanied by evidence of your identity. If this is not provided, we may contact you to ask that such evidence is forwarded before we comply with the request.

Usually, we will comply with your request without delay, within one month of receiving the request. Where requests are complex or numerous, we may contact you to inform you that an extension is required to complete the request, the maximum extension period is two months. We will normally comply with your request at no cost, however if the request is manifestly unfounded, excessive or repetitive we may contact you to request a fee. This fee must be paid in order for us to comply with the request. The fee will be determined at the relevant time and will be set at a level which is reasonable in the circumstances.

In addition, we may also charge a reasonable fee if you request further copies of the same information.

When you make a subject access request, you will be informed of:

* whether or not your data is processed and the reasons for the processing of your data;
* the categories of personal data concerning you;
* where your data has been collected from if it was not collected from you;
* anyone who your personal data has been disclosed to or will be disclosed to, including anyone outside of the EEA and the safeguards utilised to ensure data security;
* how long your data is kept for (or how that period is decided);
* your rights in relation to data rectification, erasure, restriction of and objection to processing;
* your right to complain to the Information Commissioner if you are of the opinion that your rights have been infringed;
* the reasoning behind any automated decisions taken about you.

GWT may refuse to deal with your subject access request if it is manifestly unfounded or excessive, or if it is repetitive. Where it is our decision to refuse your request, we will contact you without undue delay, and at the latest within one month of receipt, to inform you of this and to provide an explanation. You will be informed of your right to complain to the Information Commissioner and to a judicial remedy.

GWT may also refuse to deal with your request, or part of it, because of the types of information requested. For example, information which is subject to legal privilege or relates to management planning is not required to be disclosed. Where this is the case, we will inform you that your request cannot be complied with and an explanation of the reason will be provided.

The right to ‘correction’

If you discover that the data GWT hold about you is incorrect or incomplete, you have the right to have the data corrected. You should make a request for correction in writing to GWT’s Data Protection Officer.

Usually, we will comply with a request to rectify data within one month unless the request is particularly complex in which case we may write to you to inform you we require an extension to the normal timescale. The maximum extension period is two months.

You will be informed if we decide not to take any action as a result of the request. In these circumstances, you are able to complain to the Information Commissioner and have access to a judicial remedy.

Third parties to whom the data was disclosed will be informed of the rectification.

The right of ‘erasure’

In certain circumstances, GWT is required to delete the data we hold on you. Those circumstances are:

* where it is no longer necessary for us to keep the data;
* where we relied on your consent to process the data and you subsequently withdraw that consent. Where this happens, we will consider whether another legal basis applies to our continued use of your data;
* where you object to the processing (see below) and the Company has no overriding legitimate interest to continue the processing;
* where we have unlawfully processed your data;
* where we are required by law to erase the data.

You should make a request for erasure in writing to GWT’s Data Protection Officer using the Right to Data Erasure Form (Appendix 3). We will consider each request individually, however, you must be aware that processing may continue under one of the permissible reasons. Where this happens, you will be informed of the continued use of your data and the reason for this.

Third parties to whom the data was disclosed will be informed of the erasure where possible unless to do so will cause a disproportionate effect on us.

The right of ‘restriction’

You have the right to restrict the processing of your data in certain circumstances. GWT will be required to restrict the processing of your personal data in the following circumstances:

* where you tell us that the data we hold on you is not accurate. Where this is the case, we will stop processing the data until we have taken steps to ensure that the data is accurate;
* where the data is processed for the performance of a public interest task or because of our legitimate interests and you have objected to the processing of data. In these circumstances, the processing may be restricted whilst we consider whether our legitimate interests mean it is appropriate to continue to process it;
* when the data has been processed unlawfully;
* where we no longer need to process the data but you need the data in relation to a legal claim.

You should make a request for restriction in writing to GWT’s Data Protection Officer. Where data processing is restricted, we will continue to hold the data but will not process it unless you consent to the processing, or processing is required in relation to a legal claim.

Where the data to be restricted has been shared with third parties, we will inform those third parties of the restriction where possible unless to do so will cause a disproportionate effect on us. You will be informed before any restriction is lifted.

The right to data ‘portability’

You have the right to obtain the data that GWT process on you and transfer it to another party. Where our technology permits, we will transfer the data directly to the other party.

Data which may be transferred is data which:

* you have provided to us; and
* is processed because you have provided your consent or because it is needed to perform the employment contract between us; and
* is processed by automated means.

If you wish to exercise this right, please speak to your manager. GWT will respond to a portability request without undue delay, and within one month at the latest unless the request is complex or we receive a number of requests in which case we may write to you to inform you that we require an extension and reasons for this. The maximum extension period is two months. We will not charge you for access to your data for this purpose.

You will be informed if we decide not to take any action as a result of the request, for example, because the data you wish to transfer does not meet the above criteria. In these circumstances, you are able to complain to the Information Commissioner and have access to a judicial remedy.

The right to data portability relates only to data defined as above. You should be aware that this differs from the data which is accessible via a Subject Access Request.

The right to ‘object’

You have a right to require us to stop processing your data; this is known as data objection. You may object to processing where it is carried out:

* in relation to the Company’s legitimate interests;
* for the performance of a task in the public interest;
* in the exercise of official authority; or
* for profiling purposes.

You should make a request to object in writing to GWT’s Data Protection Officer.

In some circumstances we will continue to process the data you have objected to. This may occur when:

* we can demonstrate compelling legitimate reasons for the processing which are believed to be more important than your rights; or
* the processing is required in relation to legal claims made by, or against, us.

If the response to your request is that we will take no action, you will be informed of the reasons.

Right not to have automated decisions made about you

You have the right not to have decisions made about you solely on the basis of automated decision making processes where there is no human intervention, where such decisions will have a significant effect on you. At the time of writing (December 2019) automated decisions to profile personal data are not made at all by GWT.

However, we may carry out automated decision making with no human intervention in the future and in the following circumstances:

* when it is needed for entering into or the carrying out of a contract with you;
* when the process is permitted by law;
* when you have given explicit consent.

In circumstances where we use special category data, for example, data about your health, sexual orientation, race, ethnic origin, political opinion, religion, and trade union membership the Company will ensure that one of the following applies to the processing:

* you have given your explicit consent to the processing; or
* the processing is necessary for reasons of substantial public interest.

Staff have the right to be informed and to object if this situation should change.

Consent

Where you have provided consent to our use of your data, you also have the right to withdraw that consent at any time. This means that we will stop processing your data.

Making a Complaint

If you would like to make an internal complaint then please do so in triplicate to the Data Protection Officer, your line manager and the CEO. You are also entitled to submit a written complaint to the Information Commissioner (ICO) at any point in the complaints process; before, during or after any internal investigation. You can contact the ICO at Information Commissioner's Office, Wycliffe House, Water Lane, Wilmslow, Cheshire SK9 5AF or by telephone on 0303 123 1113 (local rate) or 01625 545 745.

Data Protection Compliance

Our Data Protection Officer is:

Sarah Coleman [scoleman@gwentwildlife.org](mailto:scoleman@gwentwildlife.org)

Gwent Wildlife Trust, Chestnut Suite, Mamhilad House, Mamhilad Park Estate, Pontypool, NP4 0HZ

01600 740600

**Appendix 1 - Subject Access Request Procedure**

**Scope**

All personal data processed by GWT is within the scope of this procedure. Data subjects are entitled to obtain:

* Confirmation as to whether GWT is processing any personal data about that individual;
* Access to their personal data;
* Any related information.

**Responsibilities**

* The GDPR lead is responsible for the application and effective working of this procedure, and for reporting to the information owner on Subject Access Requests (SARs).
* The GDPR lead is responsible for handling all SARs.

**Procedure**

* Subject Access Requests are made using the Subject Access Request Form (Appendix 2).
* The data subject provides GWT with evidence of their identity, in the form of a current passport or driving license, and the signature on the identity must be cross-checked to that on the application form.
* The data subject specifies to GWT which data they seek information regarding; on their subject access request (SAR). The data subject can request all data held on them.
* GWT records the date that the identification checks were conducted and the specification of the data sought.
* GWT provides the requested information to the data subject within 28 days from this recorded date. Extensions to this period may be allowed under GDPR Article 12 (3).
* Once received, the subject access request (SAR) application is immediately forwarded to the GDPR lead, who will ensure that the requested data is collected within the specified time frame.
* Collection entails:
* Collecting the data specified by the data subject, or
* Searching all databases and all relevant filing systems (manual files) in GWT, including all back up and archived files (computerised or manual) and all email folders and archives. Data migration means that a new data structure is currently being created and will be in place by 31st July 2022. The GDPR lead will then maintain a data map that identifies where all data in GWT will be stored.
* The GDPR lead maintains a record of requests for data and of its receipt, including dates.
* The GDPR lead reviews subject access requests from a child. Before responding to a SAR of the child data subject the GDPR lead considers their ability to make the request by adequately explaining any implications of sharing their personal data.
* The GDPR lead reviews all documents that have been provided to identify whether any third parties are present in it, and either removes the identifying third party information from the documentation or obtains written consent from the third party for their identity to be revealed.
* If any of the requested data is being held or processed under one of the following exemptions, it does not have to be provided:
* National security
* Crime and taxation
* Health
* Education
* Social Work
* Regulatory activity
* Journalism, literature and art
* Research history and statistics
* Publicly available information
* Corporate finance
* Examination marks
* Examination scripts
* Domestic processing
* Confidential references
* Judicial appointments, honours and dignities
* Crown of ministerial appointments
* Management forecasts
* Negotiations
* Legal advice and proceedings
* Self-incrimination
* Human fertilization and embryology
* Adoption records
* Special educational needs
* Parental records and reports
* In the event that a data subject requests GWT to provide them with the personal data stored by the controller/processor, then GWT will provide the data subject with the requested information in electronic format, unless otherwise specified. All of the items provided to the data subject are listed on an accompanying letter.
* In the event that a data subject requests what personal data is being processed then GWT provides the data subject with the following information:
* Purpose of the processing
* Categories of personal data
* Recipient(s) of the information, including recipients in third countries or international organisations
* How long the personal data will be stored
* The data subject’s right to request rectification or erasure, restriction or objection, relative to their personal data being processed.
  + GWT removes personal data from systems and processing operations as soon as a request for erasure has been submitted by the data subject.
  + GWT contacts and communicates with other organisations, where the personal data of the data subject is being processed, to cease processing information at the request of the data subject.
  + GWT takes appropriate measures without undue delay in the event that the data subject has: withdrawn consent; objects to the processing of their personal data in whole or part; no longer under legal obligation and/or has been unlawfully processed.
* Inform the data subject of their right to lodge a complaint with the supervisory authority in line with the complaints procedure.
* Information on the source of the personal data if it hasn’t been collected from the data subject.
* Inform the data subject of any automated decision-making.
* If and where personal data has been transferred and information on any safeguards in place.

**Appendix 2 - Subject Access Request Form**

|  |
| --- |
| **Name:** |
| **Daytime telephone number:** |
| **Email:** |
| **Address:** |
| **Employee number:** |
| By completing this form, you are making a request under the General Data Protection Regulation (GDPR) for information held about you by Gwent Wildlife Trust that you are eligible to receive. |
| **Required information (and any relevant dates):** |
| By signing below, you indicate that you are the individual named above. The organisation cannot accept requests regarding your personal data from anyone else, including family members. We may need to contact you for further identifying information such as viewing your passport or driving licence before responding to your request. You warrant that you are the individual named and will fully indemnify us for all losses, cost and expenses if you are not.  Anthony Cook, Gwent Wildlife Trust, Mamhilad House, Mamhilad Park Estate, Pontypool, NP4 0HZ.  Tel: 01600 740600, Email: acook@gwentwildlife.org  Please allow 28 days for a reply. |
| **Data subject's signature:** |
| **Date:** |

**Appendix 3 - Right to Data Erasure Form**

You are entitled to request us to erase any personal data we hold about you under EU General Data Protection Regulation (GDPR).

We will do our best to respond promptly and in any event within one month of the following:

* Our receipt of your written request; or
* Our receipt of any further information we may ask you to provide to enable us to comply with your request, whichever happens to be later.

The information you supply in this form will only be used for the purposes of identifying the personal data you are requesting that we erase and responding to your request. You are not obliged to complete this form to make a request, but doing so will make it easier for us to process your request quickly.

**Section 1: Details of the person requesting information**

Full name:

Address:

Contact telephone number:

Email address:

**Section 2: Are you the data subject?**

Please tick the appropriate box and read the instructions that follow it.

**Yes: I am the data subject. I enclose proof of my identity (see below),** (**please go to section 4**).

**No:**  I am acting on behalf of the data subject. I have enclosed the data subject’s written authority and proof of the data subject’s identity and my own identity (see below). (**Please go to section 3**).

To ensure we are erasing the data of the right person we require you to provide us with proof of your identity and of your address. Please supply us with a photocopy or scanned image (do not send originals) of one or both of the following:

* Proof of identity: Passport, photo driver’s license, national identity card, birth certificate.
* Proof of address: Utility bill, credit card statement (no more than 3 months old); current driver’s license.

If we are not satisfied you are who you claim to be, we reserve the right to grant your request.

**Section 3: Details of the data subject (if different from section 1).**

Full name:

Address:

Contact telephone number:

Email address:

**Section 4: Reason for erasure request**

Given the sensitive nature of erasing personal data, GDPR article 17(1) requires certain conditions to be met before a request may be considered. Please supply us with the reason you wish your data to be erased and please attach any justifying documents to this application.

Please tick the appropriate box.

 You feel your personal data is no longer necessary for the purpose for which we originally collected it.

 You no longer consent to our processing of your personal data.

 You object to our processing of your personal data as is your right under article 21 of the GDPR.

 You feel your data has been unlawfully processed.

 You feel we are subject to a legal obligation of the EU or Member State that requires the erasure of your personal data.

 You are a child, you represent a child, or you were a child at the time of the data processing and you feel your personal data was used to offer you information services.

**Section 5: What information do you wish to erase?**

Please describe the information you wish to erase. Please provide any relevant details you think will help us identify the information. Providing the URL for each link you wish to be removed (if relevant) would be helpful.

Also please explain, if it is not abundantly clear, why the linked page is about you or the person you are representing on this form. (Enter N\A if not relevant).

Please note that in certain circumstances, where erasure would adversely affect the freedom of expression, contradict a legal obligation, act against the public interest in the area of scientific or historical research, or prohibit the establishment of a legal defence or exercise of other legal claims, we may not be able to erase the information you requested in accordance with Article 17(3) of the GDPR. In such circumstances you will be informed promptly and given full reasons for that decision.

While in most cases GWT will be happy to erase the personal data you request, we nevertheless reserve the right, in accordance with Article 12(5) of the GDPR, to charge a fee or refuse the request if it is considered to be “manifestly unfounded or excessive”.

However, we will make every effort to provide you with the erasure of your personal data if suitable.

**Section 6: Declaration**

Please note that any attempt to mislead may result in prosecution.

I confirm that I have read and understood the terms of this subject access form and certify that the information given in this application to ­­­­­­­­­­­­­­­­­\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ is true.

I understand that it is necessary for \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ to confirm my/the data subject’s identity and it may be necessary to obtain more detailed information in order to locate the correct personal data.

Signed ……………………………………………

Date ……………………………………………

**Documents which must support this application:**

* **Evidence of your identity (see section 2)**
* **Evidence of the data subject’s identity (if different from the above)**
* **Authorization from the data subject to act on their behalf (if applicable)**
* **Justification for erasure of data (see section 4)**