Privacy Notice – Graduate Programme Wales

Last reviewed September 2020

Data Controller:	Graduate Programme Wales "GPW" *(sponsored by the Welsh Contact Centre Forum Ltd)*
Data Protection Officer:	Robert Jennings – Rob@wccf.uk

Graduate Programme Wales (GPW) collects and processes personal data for the purposes of recruitment, whether you are applying for a place on the Graduate Programme or applying for a role on the Graduate Programme's Management Team. GPW also collects and processes personal data relating to its graduates, to manage the employment relationship and to satisfy our contractual and legal responsibilities under the governance structure of the Programme.

GPW is committed to:

- Being transparent about how it collects and uses data.
- Meeting its data protection obligations in accordance with the principles of the General Data Protection Regulation 2016 (GDPR) and the Data Protection Act 2018 (DPA), which both came into effect on in the UK on 25th May 2018.

Full details relating to Data Protection and the internal policies and controls GPW has in place to ensure the security and confidentiality of data, can be found in our Data Security Policy – a copy of which is available upon request from the Data Protection Officer.

Please be advised that should any amendments be required to this privacy notice; a revised privacy notice will be available to download from the Buzz Wales website.

What information does GPW collect?

GPW collects and processes a range of information about you. This includes:

- your name, address and contact details, including email address and telephone number, date of birth and gender;
- the terms and conditions of your employment;
- details of your qualifications, skills, experience and employment history, including start and end dates, with previous employers and with GPW;
- payroll and salary information;
- your national insurance number, information about your nationality and entitlement to work in the UK;
- equal opportunities monitoring information, including (but not limited to) information about your ethnic origin;
- information about whether or not you have a disability for which GPW needs to make reasonable adjustments;

- assessments of your performance, including performance reviews, training plans, performance improvement plans, MSc grades/progress reports (graduates on Programme only) and other related correspondence;
- details of any disciplinary or grievance procedures in which you have been involved, including any warnings issued to you and related correspondence;
- your photo - full rights to use professional images resulting from photography/video filming instructed by GPW, and approved reproductions or adaptations of the images for publicity or other purposes to help achieve the programme aims. This might include (but is not limited to), the right to use them in their printed and online publicity, social media, press releases and funding applications. We will ask for your prior written consent for your participation in any marketing related photography or filming;
- any marketing or publicity materials which contain your photo or videos may be used after your participation in the Graduate Programme has ended.
- criminal records data – this will be collected and processed by your host employer. this is usually completed as due diligence when starting your new placement in the form of Criminal Records Bureau checks;
- employment credit checks – these may be completed by your host employer as part of their due diligence when starting your placement with them.
- any case studies that you agree to pen during the course of your time with GPW, in connection with GPW or Consortium Employers shall remain the property of the GPW. You will therefore, relinquish any rights or request any payment in return.

WGP may collect this information in a variety of ways. For example, data might be collected through application forms or CVs; obtained from your passport or other identity documents; from correspondence with you; or through interviews, meetings or other forms of assessment.

Please note that in response to the 2020 COVID-19 Pandemic, many of our recruitment processes have now been transferred online rather than being in person, mainly through the use of Microsoft Teams. Please be advised that such calls may be recorded as part of the recruitment process for evaluation purposes post-assessment. Written consent will be requested for this prior to your participation. Regardless of whether successful in gaining a placement with GPW, this will be deleted six months after a decision regarding your application has been reached.

Please be advised that depending on who you are as a data subject, not all forms of information mentioned above will need to be collected and processed about you. For example, if you are applying for a position on the graduate programme we will only collect and process information that is necessary and relevant to process your job application.

Any information provided by you will be used to enable the Graduate Programme's Management Team to create a computer and paper record for your personal, employment and development details.

Data will be stored in a range of different places, including in your individual graduate file, in WGP's management systems and in other IT systems (including email).

This information will be kept securely and will be processed in accordance with the principles of the GDPR and the DPA. Data will be shared confidentially with the Welsh Contact Centre

Forum as the Programme Manager, the Wales European Funding Office (WEFO) as sponsors of the project, relevant consortium employers and University of South Wales.

Please be advised that data collected and processed by WEFO, University of South Wales, and consortium employers will be done so according to their own policies and procedures. If you would like to know more regarding their data protection policies, please refer to their privacy notices and data protection procedures.

Why does GPW process personal data?

GPW has a legitimate interest in processing personal data before, during and after the end of the employment relationship. Processing personal data allows GPW to:

- run recruitment and promotion processes;
- maintain accurate and up-to-date individual graduate records and contact details, and records of contractual and statutory rights;
- operate and keep a record of graduate performance and related processes, to plan for career development, and for placement rotation planning purposes;
- ensure effective general administration; and
- Maintain and promote equality.

In some cases, GPW needs to process data to ensure that it is complying with its legal obligations. For example, the collection and processing of personal data by WGP is required to:

- **Satisfy WEFO audit requirements** – As the Graduate Programme is partly funded by WEFO, we are legally obliged to submit personal data to:

  a) Evidence your eligibility to join the Graduate Programme. Information required to do this includes various forms of ID (passport etc.) and evidence of previous qualifications.
  b) Evidence the financial costs of your placement on the Graduate Programme. We are legally obliged to collect and process your payroll data to demonstrate to WEFO that costs are real and genuine.

- **Satisfy employment law requirements** – To satisfy employment law requirements, information regarding your right to work in the UK will also need to be processed.

Some special categories of personal data, such as information about health or medical conditions, are processed to carry out employment law obligations (such as those in relation to graduates with disabilities). It will also be processed in order to record and monitor equal opportunities, diversity, and inclusivity. Information of this nature will not be disclosed without your prior written consent unless we are legally obliged to act without such consent.

Where GPW processes other special categories of personal data, such as information about ethnic origin, this is done for the purpose of equal opportunities, diversity and inclusivity monitoring. Information of this nature is also reported to WEFO who use the condition cited below (Article 9 of GDPR) for processing special categories of personal data:

"Processing is necessary for reasons of substantial public interest, based on Union or Member State law which shall be proportionate to the aim pursued, respect the essence of the right to data protection and provide for suitable and specific

measures to safeguard the fundamental rights and the interests of the data subject"

Qualifying Disclosures

Qualifying disclosures are disclosures of information it is reasonably believed (and it is in the public interest) that one or more of the following matters is either happening, has taken place, or is likely to happen in the future.

- A criminal offence
- The breach of a legal obligation
- A miscarriage of justice
- A danger to the health and safety of any individual
- Damage to the environment
- Deliberate attempt to conceal any of the above.

As a graduate, if you intend to make a disclosure it should be made to your employer first, or if you feel unable to use the organisation's procedures, the disclosure should be made to a prescribed person, so that employment rights are protected. If you intend to make a disclosure in relation to any of the matters cited above, you will be doing so on the grounds of vital interests, legal obligation or legitimate interests depending on which is most relevant. These are all legal bases under the GDPR and DPA.

If graduates bring information about any wrongdoing to the attention of their host employer or GPW, they are protected in certain circumstances under the Public Interest Disclosure Act 1998. Which is commonly referred to as 'blowing the whistle'. The law that protects whistle-blowers is for the public interest - so people can speak out if they find malpractice in an organisation.

Please be advised that if GPW, WEFO, Consortium Employers or the University of South Wales reasonably believe that a qualifying disclosure is required in response to any of the matters cited above, they will be done so in line with provisions under the GDPR, DPA, and/ or the Public Interest Disclosure Act 1998.

Who has access to data?

GPW is managed and operated by employees of the Welsh Contact Centre Forum Ltd (WCCF), as the parent company and primary sponsor of the project.

Your information may be shared internally, between members of the Graduate Programme's Management Team and Welsh Contact Centre Forum (WCCF) colleagues, who have a requirement to access this information for the proper performance of their duties. They are bound by contractual agreements and professional obligations to protect the confidentiality of such information.

WGP also shares your data with various third parties, who are all direct stakeholders of the Programme:

1. **Wales European Funding Office (WEFO)**

   The Programme is partly funded by WEFO; therefore, we are required to regularly report statistical data and comply with their audit requirements. Reports are created by GPW using records of graduates' personal, employment and payroll details.

2. **Participating Consortium Employers**

   GPW shares selected data with the company you are directly employed by on placement rotation (i.e. members of the company's HR/recruitment team and/or your line manager). This data is provided in order for the company to enter a contract of employment with you, and to facilitate and manage the ongoing employment relationship throughout the duration of your fixed term contract with them. This includes (but not limited to) provision of data prior to employment to enable the company to obtain pre-employment references from previous employers and run necessary credit searches or criminal records checks.

3. **University of South Wales**

   GPW provides the university with graduates' basic personal data (e.g. name and contact details, previous qualifications) for the purpose of enrolment onto the MSc/post-graduate course, which is a key component of the Programme. Information is then shared throughout your studies, for us to monitor and support your progress towards completing the qualification.

Please be advised that any information that GPW controls that is shared and processed with the direct stakeholders mentioned above is done so in accordance with our written instructions. They must not process any data shared with them in a manner contravening our instructions unless they are legally obliged to do so, on the grounds of vital interests (health emergencies for example), or in the form of a qualifying disclosure as mentioned above.

If GPW process information about you on behalf of our direct stakeholders, we will do so in accordance with their written instructions unless legally obliged to do act without such instructions, if it's on the grounds of vital interests (health emergencies for example), or qualifying disclosures as mentioned above.

From time to time, GPW will also work with third parties such as consultants and external contractors to process your data. They are legally and contractually obliged to process data according to our written instructions unless they are legally obliged to act without such instructions, if it's on the grounds of vital interests (health emergencies for example), or in the form of a qualifying disclosure as mentioned above.

GPW hold information about you at premises within the United Kingdom. Information will not be shared by us to any organisation outside the European Economic area.

The only exceptions to this are the use of Microsoft Teams, DocuSign, Survey Monkey and Hubspot. While these are US based companies, they must process data in a manner compliant with the GDPR in relation to the personal data of EU citizens.

How does GPW protect data?

GPW takes the security of your data seriously. GPW has internal policies and controls in place to ensure that your data is not lost, accidentally destroyed, misused or disclosed, and is not accessed except by our employees in the proper performance of their duties.

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

For how long does GPW keep data?

GPW will hold your personal data for the duration of your employment. Thereafter, your data is retained after the end of employment and held securely for the lifetime of the Programme and used for evaluation and/ or audit purposes only.

Retention of this information is currently required until 31st December 2024, if this date is changed, our privacy notice will be updated to reflect this. When retention of this information is no longer necessary, for example when WEFO or Data Protection retention guidelines (whichever is greater) have been met, the data will be securely destroyed.

If you are unsuccessful in applying for a position on the graduate programme, this information will be held for a period of six months after a decision has been reached regarding your application. If you would like us to delete this information more quickly, please contact the GPW Project Team in writing.

You will also be provided with an option for us, as part of your application to forward your CV and contact details to consortium employers who may have their own job opportunities outside of the Graduate Programme. We will not do this without your prior consent.

Your rights

As a data subject, you have a number of rights. You can:

- **Access and obtain a copy of your data on request.** You can request a copy of the personal data we hold on record for you.
- **Withdraw consent to process your data.** This only applies where we rely on consent to process any personal data about you. Please be advised that this does not affect the lawfulness of processing before you withdraw consent.
- **Request the transfer of your data.** The ability to obtain and reuse your personal data for your own purposes across different services. The data will be formatted in a commonly used, machine-readable format. Please note that this right only applies to automated information of which you had initially provided consent for us to use or where we have used the information to perform a contract with you.
- **Require GPW to change incorrect or incomplete data.**
- **Require GPW to delete or stop processing your data**, for example where the data is no longer necessary for the purposes of processing, i.e. to fulfil its legal obligations.

- **Object to the processing of your data** where GPW is relying on its legitimate interests as the legal basis for processing.

If you would like to exercise any of these rights, please contact our Data Protection Officer on robert.jennings@wccf.uk

Should any of your details change, please inform us as soon as possible so we can update our records accordingly and ensure their accuracy.

If you choose to exercise any of the rights above, please be advised that we usually have one calendar month to respond to such requests. We have the right to request an extension of two calendar months should the request be highly complex or repetitive in nature. Should this be the case, we will write to you explaining why this is the case. Depending upon the nature of your request, we may also be required to contact WEFO.

Under certain circumstances, we also have the right to refuse requests. For example, as we have a legal obligation to adhere to WEFO and/ or European Commission audit requirements, we will be unable to delete certain forms of personal data we hold on record for you. Should we refuse any requests, we will inform you in writing within one month of your initial request explaining why this is the case. You will also be advised of your right to complain to the ICO and your right to seek a judicial remedy to enforce your rights.

If you believe that GPW has not complied with your data protection rights, you can complain to the Information Commissioner. Further information can be found at www.ico.org.uk. It would be appreciated however if you contact us in the first instance in order to address your concerns before approaching the ICO.

What if you do not provide personal data?

Certain information, such as contact details and your right to work in the UK, must be provided to enable GPW to manage the employment relationship. If you do not provide other information, this will hinder WGP's ability to administer the rights and obligations arising as a result of the employment relationship efficiently. As we will be unable to verify your right to work in the UK and satisfy out legal obligations as part of this Programme, we will have the legal right to withdraw any job offer or enrolment onto the Graduate Programme. If this is the case, you will be notified in writing.