ORCI GDPR Policy

1. Overview

The ORCi & its members take the security and privacy of data seriously. We need to gather and use information or 'data' about you as part of our business. We intend to comply with our legal obligations under the Data Protection Act 2018 (the '2018 Act') and the EU General Data Protection Regulation ('GDPR') in respect of data privacy and security. We have a duty to notify you of the information contained in this policy.

This policy applies to current and former employees, volunteers, workers, contractors and anyone who works under our jurisdiction. If you fall into one of these categories, then you are a 'data subject' for the purposes of this policy.

- We will utilise this policy for the purpose of job applicants, customers, suppliers and other categories of data subject.
- We have measures in place to protect the security of your data.
- We will hold data for as long as necessary for the purposes for which we collected it.

This policy is intended that this policy is fully compliant with the 2018 Act and the GDPR. If any conflict arises between those laws and this policy, the ORCi and its members intends to comply with the 2018 Act and the GDPR.

2. Data Protection Principles

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 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; and
- be processed securely.

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

3. How we define personal data

'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.

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

This personal data might be provided to us by you, or someone else (such as a former employer 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 employer or other colleagues.

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, salary (including details of previous remuneration).
- 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.
- background checks such as Data Barring service (DBS)
- electronic information in relation to your use of IT systems/swipe cards/telephone systems.

- your images (whether captured on CCTV, by photograph or video).
- any other category of personal data which we may notify you of from time to time.

4. How will we process your personal data?

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

We will use your personal data for:

- performing the contract of employment (or services) between us.
- complying with any legal obligation.

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.

5. Examples of when we might process your personal data.

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). For example:

- with another employer either within or outside our membership for genuine reasons such as employment checks
- 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 a disability.
- to monitor diversity and equal opportunities
- to monitor and protect the security (including network security) of our other staff, customers and others.
- to monitor and protect the health and safety of you, our other staff, customers and third parties.
- to pay you in accordance with the contract between us
- 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 or us.
- running our business and planning for the future

- the prevention and detection of fraud or other criminal offences
- to defend us in respect of any investigation or litigation and to comply with any court or tribunal orders for disclosure.
- for any other reason which we may notify you of from time to time.
- 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.
- For any professional agencies, such as the police, where we are obliged to share your data.

6. Sharing your personal data

Sometimes we might share your personal data with group companies or our contractors and agents to carry out our obligations under our contract with you or for our legitimate interests. We will not do this without your permission.

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.

7. How should we process personal data?

- Everyone who works for, or on behalf of the ORCi has some responsibility for ensuring data is collected, stored and handled appropriately.
- We will not share personal data informally.
- You should keep personal data secure and not share it with unauthorised people.
- 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.
- You should not make unnecessary copies of personal data and should keep and dispose of any copies securely.
- You should use strong passwords.
- You should lock your computer screens when not at your desk.
- Personal data should be encrypted before being transferred electronically to authorised external contacts.
- Consider anonymising data or using separate keys/codes so that the data subject cannot be identified.
- Do not save personal data to your own personal computers or other devices.
- Personal data should never be transferred outside the European Economic Area except in compliance with the law and authorisation of the Data Protection Officer.

- You should lock drawers and filing cabinets. Do not leave paper with personal data lying about.

- You should not take personal data away from Company's premises without authorisation.

- Personal data should be disposed of securely when you have finished with it.

- You should ask for help from your superior if you are unsure about data protection or if you notice any areas of data protection or security we can improve upon.

- Any deliberate or negligent breach of this policy by you may result in disciplinary action being taken against you and we may refer this to outside agencies such as the police.

- It is a criminal offence to conceal or destroy personal data which is part of a subject access request. This conduct would also amount to gross misconduct under our disciplinary procedure, which could result in your dismissal and possible criminal proceedings.

8. How to deal with data breaches

- We have 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.

- If you are aware of a data breach you must contact the ORCi immediately and keep any evidence, you have in relation to the breach.

9. Your data subject rights.

- You have the right to information about what personal data we process, how and on what basis as set out in this policy.

- You have the right to access your own personal data by requesting in writing what data we hold on to you.

- You can correct any inaccuracies in your personal data.

- 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.

- You have the right to request that we erase any aspects of your personal data that is proven to contain in-accuracies.

- 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.

- You have the right to object if we process your personal data for the purposes of direct marketing.

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

- You have the right to complain to the Information Commissioner. You can do this be 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). This website has further information on your rights and our obligations.

Created 20/08/23 v3.