GDPR Policy

(General Data Protection Regulation)

1. Definitions

1.1. Data Subject: a living individual.

1.2. Data Controller: the person or organisation that determines the means and the purpose of processing the personal data.

1.3. Legislation: includes :

(i) the Data Protection Act 1998, until the effective date of its repeal

(ii) the General Data Protection Regulation ((EU) 2016/679) (GDPR) and any national implementing laws, regulations and secondary legislation, for so long as the GDPR is effective in the UK, and

(iii) any successor and supplemental legislation to the Data Protection Act 1998 and the GDPR, in particular the Data Protection Bill 2017-2019 and the E-Privacy Directive (and its proposed replacement), once it becomes law.

1.4. Personal data: is any information that identifies a living individual (data subject) either directly or indirectly. This also includes special categories of personal data. Personal data does not include data which is entirely anonymous, or the identity has been permanently removed making it impossible to link back to the Data Subject.

1.5. Processing: is any activity relating to personal data which can include collecting, recording, storing, amending, disclosing, transferring, retrieving, using or destruction.

1.6. Special categories: this includes any personal data which reveals a data subject's, ethnic origin, political opinions, religious and philosophical beliefs, trade union membership, genetic, biometric or health data, sex life and sexual orientation.

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

2. What are the GDPR principles?

2.1. Whitehead Ross Education and Consulting (WREC) are a Data Controller. This means that we are required by law to ensure that everyone who processes personal data and special categories of personal data during the course of their work with us does so in accordance with the data protection legislation, including the GDPR principles. In brief, the principles say that:

- Personal data must be processed in a lawful, fair and transparent way.
- The purpose for which the personal information is collected must be specific, explicit and legitimate.
- The collected personal data must be adequate and relevant to meet the identified purpose.
- The information must be accurate and kept up to date.
- The personal data should not be kept in a form which permits identification of a Data Subject for longer than is necessary for the purposes for which it is used.
- The personal data must be kept confidential and secure and only processed by authorised personnel.

3. Other rules under the GDPR state that:

- The transfer of personal data to a country or organisation outside the EEA should only take place if appropriate measures are in place to protect the security of that data.
- The Data Subject must be permitted to exercise their rights in relation to their personal data.

3.1. WREC and all employees must comply with these principles and rules at all times in their information-handling practices. We are committed to ensuring that these principles and rules are followed, as we take the security and protection of data very seriously.

3.2. You must inform us immediately if you become aware that any of these principles or rules have been breached or are likely to be breached.

4. What are the lawful reasons under which we process personal data?

4.1. WREC will only process personal data where the business has a lawful basis (or bases) to process that information. The lawful basis may be any one of the following reasons or a combination of:

- Consent has been obtained the Data Subject to process their personal data for specified purposes.
- Where we need to perform the contract we have entered into with the Data Subject, either for employment or commercial purposes.
- Where we need to comply with a legal obligation.
- Where it is necessary for our legitimate interests (or those of a third party) and the interests and fundamental rights of the Data Subject do not override those interests.

4.2. There are other rare occasions where you may need to process the Data Subjects' personal information, these include:

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

5. Privacy Notices

5.1. Before we collect or process personal data directly from a Data Subject, we will ensure that an appropriate privacy notice has been issued to the Data Subject. The content of the privacy notice will provide accurate, transparent and unambiguous details of the lawful and fair reason for why we are processing the data. It will also explain how, when and for how long we propose to process the Data Subjects' personal information.

6. Purpose Limitation

6.1. When we collect personal information, we will set out in the privacy notice how that information will be used. If it becomes necessary to use that information for a reason other than the reason which we have previously identified, we will stop processing that information. However, in limited circumstances we will continue to process the information provided that the new reason for processing the personal information remains compatible with the original lawful purpose.

7. Adequate and relevant

7.1. We will only process personal data where we have been authorised to do so because it relates to a service user accessing one of our programmes or an employee's work. We will not collect, store or use unnecessary personal data and we will ensure that personal data is deleted, erased or removed within WREC's retention guidelines. We will not process or use personal data for non-WREC related purposes.

7.2. WREC will review its records and in particular service user records and employees' personnel files on a regular basis to ensure they do not contain a backlog of out-of-date or irrelevant information and to check there are lawful reasons requiring information to continue to be held.

8. Accurate and kept up to date

8.1. If your personal information changes, for example you change address, you must inform the programme coordinator as soon as practicable so that WREC's records can be updated. WREC will not be responsible for any inaccurate personal data held on its systems where you have failed to notify it of the relevant change in circumstances.

9. Kept for longer than is necessary

9.1. Different categories of personal data will be retained for different periods of time, depending on legal, operational and financial requirements. Any data which WREC decides it does not need to hold for a particular period of time will be destroyed in accordance with its retention of data policy.

10. Kept confidential and secure

- WREC has in place appropriate technical and organisational measures to protect against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to data.
- Where WREC provides staff with code words or passwords to be used before releasing personal information, for example by telephone, staff must strictly follow WREC's requirements in this regard.
- Staff will only transmit personal information between locations by e-mail if a secure network is in place, for example, if an encryption is used for e-mail.
- Staff will ensure that any personal data which we hold is kept securely, either in a locked filing cabinet or, if it is computerised, it is password protected so that it is protected from unintended destruction or change and is not seen by unauthorised persons.
- Staff will not access another employee's records without authority as this will be treated as gross misconduct and it is also a criminal offence.
- Staff will not write down (in electronic or hard copy form) opinions or facts concerning a Data Subject which would be inappropriate to share with that Data Subject.
- Staff will not remove personal information from the workplace with the intention of processing it elsewhere unless this is necessary to enable you to carry out your job duties and has been authorised by their line manager.
- Staff will ensure that when working on personal information as part of their job duties when away from their workplace and with the authorisation of their line manager, they continue to observe the terms of this policy and the data protection legislation, in particular in matters of data security.

- Staff will ensure that hard copy personal information is disposed of securely in our confidential waste cabinets.
- Manual personnel files and Data Subject files are confidential and are stored in locked cabinets. Only authorised employees have access to these files. These will not be removed from their normal place of storage without good reason.
- Data stored on memory sticks, discs, portable hard drives or other removable storage media must be kept in locked filing cabinets.
- Data held on computers are stored confidentially and protected by password.
- WREC has network back-up procedures to ensure that data on computers cannot be accidentally lost or destroyed.

11. Transfer to another country

11.1. We do not have a need to transfer data outside of the European Economic Area (EEA).

12. The Data Subject rights

12.1. The Data Subject must be permitted to exercise their rights in relation to their personal data. Under the GDPR, subject to certain legal limitations, Data Subjects have available a number of legal rights regarding how their personal data is processed. At any time, a Data Subject can request that WREC should take any of the following actions, subject to certain legal limitations, with regard to their personal data:

- Allow access to the personal data
- Request corrections to be made to data
- Request erasure of data
- Object to the processing of data
- Request that processing restrictions be put in place
- Request a transfer of personal data
- Object to automated decision making
- Right to be notified of a data security breach

12.2. There are different rules and timeframes that apply to each of these rights. Staff will follow WREC's policies and procedures whenever they process or receive a request in relation to any of the above rights.

13. Responding to a Data Subject request

13.1. Staff will follow WREC's Data Subject access procedure which details how to deal with requests, and it describes the circumstances where a fee may be charged. In following these procedures staff will:

- Always verify the identity of the person making a Data Subject request and the legitimacy of the request.
- Not give out confidential personal information unless they have received the appropriate consent from the Data Subject in writing. Staff will seek explicit written consent to process the Data Subject request and ensure that they keep a clear audit trail of the request and their response.
- Not share personal information with a third party, unless the Data Subject has given their explicit prior consent to the sharing of their information. A third party is anyone who is not the actual Data Subject and can include a family member of the Data Subject.
- Take great care not to accidentally share information with an unauthorised third party.
- Be aware that those seeking information sometimes use deception in order to gain access to it.

14. Categories of information

14.1. During the course of their employment staff will be required to process personal data which falls into different categories, general personal data and special categories of personal data. All data should be processed in accordance with the privacy notice and at all times in a confidential manner. However, where that data is classed as a special category extra care should be taken to ensure the privacy and security of that data. This means that staff should maintain a high level of security and they should only share this data with those who are also authorised to process that data.

14.2. Staff may be asked to process information in relation to criminal convictions. This should be processed with the highest degree of confidentiality and in accordance with any data protection legislation and privacy notices that are in force in our business.

14.3. If you are unsure about how you should process general personal data or special categories of personal data, you must contact the Data Protection Officer, Ian Ross.

15. When will you need to seek consent?

15.1. We will require consent from a Data Subject in order to process personal data or special categories of data. Staff will be provided with training and details of which circumstances consent is needed and the type of consent that should be sought.

15.2. Staff must not compel a Data Subject to provide written consent. Giving consent will always be a decision made by freewill and choice. Consent can be withdrawn at any time without any reason provided. You must not subject a Data Subject to a sanction or detriment as a consequence of withdrawing consent.

16. Action to be taken in the event of a data protection breach

16.1. A personal data breach will arise whenever any personal data is lost, destroyed, corrupted or disclosed; if someone accesses the data or passes it on without proper authorisation; or if the data is made unavailable and this unavailability has a significant negative effect on a Data Subject.

16.2. Staff must follow WREC's Data Breach Policy which includes immediately informing the Data Protection Officer so that steps can be taken to:

- Contain the breach,
- Assess the potential adverse consequences for individuals, based on how serious or substantial these are, and how likely they are to happen, and
- To limit the scope of the breach by taking steps to mitigate the effects of the breach.

16.3. The Data Protection Officer will determine within 72 hours the seriousness of the breach and if the Information Commissioner's Office (ICO) and/or Data Subjects need to be notified of the breach.

17. Record keeping

17.1. As we have fewer than 250 employees, we only need to document processing activities that:

- are not occasional; or
- could result in a risk to the rights and freedoms of individuals; or
- involve the processing of special categories of data or criminal conviction and offence data.

18. Training

18.1. All employees that handle personal information of individuals must have a basic understanding of the data protection legislation, including the GDPR. Staff with duties such as computer and internet security, marketing and database management may need specialist training to make them aware of particular data protection requirements in their work area.

18.2. We will provide staff with continuous training and updates on how to process personal data in a secure and confidential manner and in accordance with the spirit of the data protection legislation, including the GDPR. Staff will be required to attend all training and to keep themselves informed and aware of any changes made to privacy notices, consent procedures and any other policies and procedures associated with our internal processing of personal data.

18.3. We will regularly review all your data processing activities and ensure that we are acting in accordance with the most current best practice and legal obligations in relation to data security and confidentiality.

19. Sharing personal data

19.1. We may share personal data internally as is necessary. Staff will always ensure that personal data is only shared with authorised persons and is shared in accordance with the purposes stated in any privacy notice or consents. Extra care and security must be taken when sharing special categories of data or transferring data outside of WREC to a third party.

20. Direct Marketing

20.1. We are subject to specific rules under the GDPR in relation to marketing our services. Data Subjects have the right to reject direct marketing and we will ensure that Data Subjects are given this option at first point of contact. When a Data Subject exercises their right to reject marketing you must desist immediately from sending further communications.

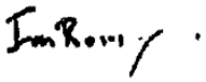
21. Complaints

21.1. If a service user believes that this policy has been breached by a member of staff to exercise all relevant rights, queries or complaints please in the first instance contact our Data Protection Officer, Ian Ross.

22. Changes to this policy

22.1. We reserve the right to change this policy at any time to ensure we are following the correct procedures.

Signed:



Ian Ross
Managing Director

Date: 10th May 2023