# Future Wolverton Limited Data Retention, Storage, Usage and Protection Policy and Procedures February 2024

1. Introduction
    1. Future Wolverton sometimes enters into contracts that require it to keep and process certain information about individuals.
    2. The organisation also needs to keep and process information about workers so that they can be recruited and paid, and legal obligations to the government complied with.
    3. Future Wolverton also needs to keep records on the progress of trainees and work placement students so that, for example, reports can be given to funders or sponsors.
    4. Future Wolverton also needs to communicate with members, customers and visitors using data they have supplied during their registration, purchase or visit to our websites, venues or events.
2. Terms
    1. “Personal data” means data (whether stored electronically or paper based) relating to a living individual who can be identified directly or indirectly from that data.
    2. “Processing” is any activity that involves use of personal data. It includes obtaining, recording or holding the data, organising, amending, retrieving, using, disclosing, erasing or destroying it. Processing also includes transferring personal data to third parties.
    3. Sensitive personal data includes personal data about a person’s racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, genetic, biometric, physical or mental health condition, sexual orientation or sexual life. It can also include data about criminal offences or convictions. Sensitive personal data can only be processed under strict conditions, including with the consent of the individual.
    4. Confidentiality means that only people who are authorised to use the data can access
    5. Integrity means that personal data should be accurate and suitable for the purpose for which it is processed
    6. Availability means that authorised users should be able to access the data if they need it for authorised purposes.
3. Policy
    1. Future Wolverton will maintain data security by protecting the confidentiality, integrity and availability of the personal data,
    2. Future Wolverton will take all possible care to keep personal data safe and secure
    3. Future Wolverton will cleanse data stored to reduce the data held to the minimum to meet the requirements above
    4. Future Wolverton is mindful of its duty to act in accordance with the requirements of the Data Protection Act 1998 and General Data Protection Regulations 2018.
    5. Future Wolverton will ensure that all personal data is:
        1. Processed fairly, lawfully and in a transparent manner.
        2. Collected for specified, explicit and legitimate purposes and any further processing is completed for a compatible purpose
        3. Adequate, relevant and limited to what is necessary for the intended purposes.

4. Accurate and, where necessary, kept up to date.
5. Kept in a form which permits identification
6. Kept for no longer than necessary for the intended purposes.
7. Processed in line with the individual's rights and in a manner that ensures appropriate security of the personal data, including protection against unauthorized or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.
8. Not transferred to people or organisations situated in countries without adequate protection.
9. Transferred only to a data processor that agrees to comply with these procedures and policies or has put in place similar adequate measures.

6. In accordance with the General Data Protection Requirements, Future Wolverton will only process personal data where it is required for a lawful purpose or if the individual has given their consent. Lawful purposes include (amongst others):
    1. If the processing is necessary for performing a contract with the individual: (note that, when trainees join the Work-Related Learning Programme contracts are created between the trainee and Future Wolverton and between Future Wolverton and the funder or sponsor).
    2. For compliance with a legal obligation.
    3. For the legitimate interest of the business.
7. Future Wolverton will not keep personal data longer than is necessary for the purpose or purposes for which it was collected. Future Wolverton will take all reasonable steps to destroy, or erase from our systems, all data which is no longer required for the function for which it was collected and permission to hold it obtained and will actively purge obsolete and unwanted data from time to time.
8. Future Wolverton will take appropriate security measures against unlawful or unauthorised processing of personal data, and against the accidental or unlawful destruction, damage, loss, alteration, unauthorised disclosure of or access to personal data transmitted, stored or otherwise processed.

## 4. Implementation

1. The CEO and Operations Manager will ensure that this policy is implemented and that all staff and volunteers understand their responsibilities.
2. The Data Controller and the Designated Data Controller
    1. The registered society Future Wolverton Limited as a body corporate is the Data Controller under the Data Protection Act and the Board of Future Wolverton is therefore ultimately responsible for implementation of this policy.
    2. However, a Designated Data Controller is appointed for dealing with day-to-day matters and to be the first point of contact for enquirers.
    3. The Designated Data Controller is responsible for ensuring that the Information Commissioners Office is properly notified and paid.
    4. The Designated Data Controller also includes the role of GDPR Co-ordinator.
    5. The Designated Data Controller for Future Wolverton is John Sherwood

### Procedures

1. **If personal data is collected from an individual,** they will be informed about:
    1. The purpose or purposes for which we intend to process that personal data, as well as the legal basis for the processing

2. The types of third parties, if any, with which we will share or disclose that personal data.
3. How individuals can limit our use and disclosure of their personal data
4. The period that their personal data will be stored or the criteria used to determine that period
5. Their right to request from us, as the controller, access to and rectification or erasure of personal data or restriction of processing
6. Their right to object to processing and their right to data portability
7. Their right to withdraw their consent at any time (if consent was given) without affecting the lawfulness of the processing before the consent was withdrawn (but Trainees should note that withdrawing consent might mean funding for their place on the Work-Related Learning programme may also be withdrawn)
8. The right to lodge a complaint with the Information Commissioner's Office.
9. Whether the provision of the personal data is a statutory or contractual requirement, or a requirement necessary to enter into a contract, as well as whether the individual is obliged to provide the personal data and any consequences of failure to provide the data.

2. **If Future Wolverton receives personal data about an individual from other sources,**
   1. Future Wolverton will provide them with this information as soon as possible (in addition to telling them about the categories of personal data concerned) but at the latest within 1 month.
3. **Future Wolverton will inform subjects whose personal data is processed**:
   1. That Future Wolverton is the responsible Data Controller with regard to that data.
   2. The name and contact details of the Designated Data Protection Officer.
   3. Future Wolverton will only collect personal data to the extent that it is required for the specific purpose notified to the data subject.
   4. Future Wolverton will ensure that personal data we hold is accurate and kept up to date.
   5. Future Wolverton will check the accuracy of any personal data at the point of collection. We will take all reasonable steps to destroy or amend inaccurate or out-of- date data
   6. **Future Wolverton will process all personal data in line with data subjects' rights**, in particular their right to:
      1. Confirmation as to whether or not personal data concerning the individual is being processed.
      2. Request access to any data held about them by a data controller.
      3. Request rectification, erasure or restriction on processing of their personal data
      4. Lodge a complaint with a supervisory authority.
      5. Data portability.
      6. Object to processing including for direct marketing.
4. **To maintain a secure data storage environment** Future Wolverton will:
   1. Pursue an active strategy to minimise the data held in remote storage or on workers' electronic devices
   2. Take all reasonable measures to otherwise secure digitally held or paper held data
   3. Instruct workers to move data as quickly as is reasonably possible to the higher level of security provided by the remote data storage provider

4. Instruct workers in the problems associated with the storage of personal data on external storage such as USB devices etc., which are not protected by passwords or encrypted, and actively discourage their use.

5. Methods of **disposal of redundant data**
    1. Digital data is to be deleted and over written.
    2. Paper documents are to be shredded.
    3. Digital storage devices should be reformatted when no longer required.
6. **Subject access requests**
    1. Individuals must make a formal request for information we hold about them. This must be made by email or letter.
    2. Directors or staff who receive a request should forward it to the Designated Data Controller or the CEO immediately.
    3. Future Wolverton will make no charge for the first occasion that access is requested but may make a charge of £10 per each subsequent request at its discretion.
    4. Future Wolverton aims to comply with requests for access to personal information as quickly as possible but will ensure that it is provided within 21 working days unless there is good reason for delay. In such cases, the reason for delay will be explained in writing to the data subject making the request.
    5. Individuals who request the data that we hold about them must verify their own identity before that data can be released.
    6. The Designated Data Controller, or CEO, will determine if that verification is sufficient proof of identity. If it is not then the data will not be released.
7. **Subject consent**
    1. In many cases, Future Wolverton can only process personal data with the consent of the individual.
    2. In some cases, if the data is sensitive, express consent must be obtained.
    3. Agreement to Future Wolverton processing some specified classes of personal data may be a condition of acceptance of some contracts and/or may be a condition of acceptance on the Work-Related Learning programme.
    4. Agreement to Future Wolverton processing some specified classes of personal data is a condition of employment for staff, including information about previous criminal convictions including spent convictions (because all staff work with vulnerable adults and children).
    5. If fulfilment of contractual obligation requires Future Wolverton to ask for information about particular health needs, such as allergies to particular forms of medication, or any conditions such as asthma or diabetes:
        1. Future Wolverton will only use that information in the protection of the health and safety of the individual
        2. Future Wolverton will need consent to process that information, in the event of a medical emergency, for example, therefore the individuals (or their legal guardians) concerned will be asked to sign a Consent To Process form regarding that type of information. A refusal to sign such a form may result in denial of a service or exclusion from activities.
8. **Processing sensitive personal data**
    1. Sometimes it is necessary to process information about a person's health, criminal convictions, ethnicity, gender and family details. This may be to ensure that Future Wolverton is a safe place for everyone, or to operate other policies, such as the sick pay policy or equal opportunities policy.

2. Because this information is considered sensitive, and it is recognised that the processing of it may cause particular concern or distress to individuals, workers will be asked to give express consent for Future Wolverton to do this. Offers of employment may be withdrawn if an individual refuses to consent to this without good reason.

9. **Longer term retention of personal data**
    1. Future Wolverton will keep some forms of information for longer than others, for example in compliance with the requirements of funding authorities to demonstrate that beneficiaries of a programme have met the required mix of gender, ethnicity etc. When such information is held on behalf of other organisations,
    2. Future Wolverton will abide by these requirements for the retention of that information where it has been possible to explain the requirement and obtain and record the informed consent of the individuals concerned.
10. **Responsibilities of workers** All employees must:
    1. Check that any information that they provide to Future Wolverton, in connection with their employment, is accurate and up to date.
    2. Inform Future Wolverton of any changes to information that they have provided, e.g. changes of address, as soon as possible.
    3. Check, for accuracy, the information that Future Wolverton may send out from time to time, giving details of information kept and processed about workers.
    4. Inform Future Wolverton of any errors or changes. Future Wolverton cannot be held responsible for any errors unless the worker has informed Future Wolverton about an error.
    5. Comply with these guidelines if and when, as part of their responsibilities, workers collect information about other people, (e.g. as part of a service to a customer).
    6. Data security. All workers are responsible for ensuring that:
        1. Any personal data held on laptops and other devices is kept securely
        2. Hard drives on laptops used by workers are password protected
        3. Laptops and devices holding data are backed up to external hard drives at least weekly
        4. External hard drives and backup devices are locked away when not in use
        5. Backups older than three years are permanently deleted and over written or reformatted
        6. When data is shared between workers or devices it is to be done via the secure electronic means (Google Drive)rather than by USB drives or other external drives.
        7. Documents containing customer or trainee data should be originated on cloud based applications (Google Docs) and stored in the cloud storage (Google Drive). No documents should be stored on local hard drives, external hard drives or USB drives.
        8. Data held on paper must be destroyed after seven years, or ten years if European Funding is involved, unless that data is both useful for Future Wolverton's business and still current. The use of paper based records should be actively discouraged.
        9. Personal information is not accidentally or otherwise disclosed either orally or in writing to any unauthorised third party.

10. Workers will understand that deliberate unauthorised disclosure will usually be a disciplinary matter and may be considered gross misconduct. Accidental disclosure, unless reckless, will not be considered gross misconduct but might, in some cases, be treated as a disciplinary matter.
11. Accidental disclosure should be reported, immediately it is recognised, to a line manager and then to the Designated Data Protection Officer or the CEO.

7. Compliance
    1. Compliance with the Regulations is the responsibility of all employees and volunteers.
    2. Any deliberate breach of the data protection policy may lead to disciplinary action being taken, or even a criminal prosecution. Any questions or concerns about the interpretation or operation of this policy should be taken up with the designated Data Controller or CEO.
    3. It is a condition of employment that employees will abide by the rules and policies made by the Future Wolverton from time to time. Any failure to follow this policy can therefore result in disciplinary proceedings.
    4. Any worker who considers that this policy has not been followed in respect of personal data about themselves should raise the matter with the Designated Data Controller or CEO, initially. If the matter is not resolved, it should be raised as a formal grievance.

**Last reviewed: 19th March 2025**
**Next review date: March 2026**