



Woodend Arts Limited
GDPR Policy

DATA PROTECTION POLICY

Aim and scope of policy

This policy applies to the processing of personal data in manual and electronic records kept by WAL in connection with its human resources function as described below. It also covers the Company's response to any data breach and other rights under the General Data Protection Regulation and current Data Protection Act.

This policy applies to the personal data of job applicants, existing and former employees, volunteers, placement students, workers, self-employed contractors and customers. These are referred to in this policy as relevant individuals.

"Personal data" is information that relates to an identifiable person who can be directly or indirectly identified from that information, for example, a person's name, identification number, location, online identifier. It can also include pseudonymized data.

"Special categories of personal data" is data which relates to an individual's health, sex life, sexual orientation, race, ethnic origin, political opinion, religion, and trade union membership. It also includes genetic and biometric data (where used for ID purposes).

"Criminal offence data" is data which relates to an individual's criminal convictions and offences.

"Data processing" is any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

WAL makes a commitment to ensuring that personal data, including special categories of personal data and criminal offence data (where appropriate) is processed in line with GDPR and domestic laws and all its employees conduct themselves in line with this, and other related, policies. Where third parties process data on behalf of WAL, WAL will ensure that the third party takes such measures to maintain the WAL's commitment to protecting data. In line with current data protection legislation, WAL understands that it will be accountable for the processing, management and regulation, and storage and retention of all personal data held in the form of manual records and on computers.

Types of data held

Personal data is kept in personnel files or within the WAL's HR systems. The following types of data may be held by WAL, as appropriate, on relevant individuals:

- name, address, phone numbers - for individual and next of kin
- CVs and other information gathered during recruitment
- references from former employers
- National Insurance numbers
- job title, job descriptions and pay grades
- conduct issues such as letters of concern, disciplinary proceedings
- holiday records

- internal performance information
- medical or health information
- sickness absence records
- tax codes
- terms and conditions of employment
- training details.

Relevant individuals should refer to WAL's privacy notice for more information on the reasons for its processing activities, the lawful bases it relies on for the processing and data retention periods.

Data protection principles

All personal data obtained and held by WAL will:

- be processed fairly, lawfully and in a transparent manner
- be collected for specific, explicit, and legitimate purposes
- be adequate, relevant, and limited to what is necessary for the purposes of processing
- be kept accurate and up to date. Every reasonable effort will be made to ensure that inaccurate data is rectified or erased without delay
- not be kept for longer than is necessary for its given purpose
- be 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
- comply with the relevant data protection procedures for international transferring of personal data.

In addition, personal data will be processed in recognition of an individuals' data protection rights, as follows:

- the right to be informed
- the right of access
- the right for any inaccuracies to be corrected (rectification)
- the right to have information deleted (erasure)
- the right to restrict the processing of the data
- the right to portability
- the right to object to the inclusion of any information
- the right to regulate any automated decision-making and profiling of personal data.

Procedures

WAL has taken the following steps to protect the personal data of relevant individuals, which it holds or to which it has access:

- it appoints or employs employees with specific responsibilities for:
 - a. the processing and controlling of data
 - b. the comprehensive reviewing and auditing of its data protection systems and procedures
 - c. overseeing the effectiveness and integrity of all the data that must be protected.

There are clear lines of responsibility and accountability for these different roles.

- it provides information to its employees on their data protection rights, how it uses their personal data, and how it protects it. The information includes the actions relevant individuals can take if they think that their data has been compromised in any way

- individuals' health data - to comply with health and safety or occupational health obligations towards the employee
- for Statutory Sick Pay purposes
- HR management and administration - to consider how an individual's health affects his or her ability to do their job
- the smooth operation of any employee insurance policies or pension plans.

These kinds of disclosures will only be made when strictly necessary for the purpose.

Data security

WAL adopts procedures designed to maintain the security of data when it is stored and transported.

In addition, employees must:

- ensure that all files or written information of a confidential nature are stored in a secure manner and are only accessed by people who have a need and a right to access them
- ensure that all files or written information of a confidential nature are not left where they can be read by unauthorised people
- refrain from sending emails containing sensitive work-related information to their personal email address
- check regularly on the accuracy of data being entered into computers
- always use the passwords provided to access the computer system and not abuse them by passing them on to people who should not have them
- use computer screen blanking to ensure that personal data is not left on screen when not in use.

Personal data relating to employees should not be kept or transported on laptops, USB sticks, or similar devices, unless authorised by their manager. Where personal data is recorded on any such device it should be protected by:

- ensuring that data is recorded on such devices only where necessary
- using an encrypted system – a folder should be created to store the files that need extra protection and all files created or moved to this folder should be automatically encrypted
- ensuring that laptops or USB drives are not left lying around where they can be stolen.

Failure to follow WAL's rules on data security may be dealt with via WAL's disciplinary procedure. Appropriate sanctions include dismissal with or without notice dependent on the severity of the failure.

Breach notification

Where a data breach is likely to result in a risk to the rights and freedoms of individuals, it will be reported to the Information Commissioner within 72 hours of WAL becoming aware of it and may be reported in more than one instalment.

Individuals will be informed directly if the breach is likely to result in a high risk to the rights and freedoms of that individual.

If the breach is sufficient to warrant notification to the public, the Company will do so without undue delay.

Training

New employees must read and understand the policies on data protection as part of their induction.

All employees receive training covering basic information about confidentiality, data protection and the actions to take upon identifying a potential data breach.

The nominated data controller/auditors/protection officers for the Company are trained appropriately in their roles under data protection legislation.

All employees who need to use the computer system are trained to protect individuals' private data, to ensure data security, and to understand the consequences to them as individuals and WAL of any potential lapses and breaches of WAL's policies and procedures.

Records

WAL keeps records of its processing activities including the purpose for the processing and retention periods in its HR data record. These records will be kept up to date so that they reflect current processing activities.

Data protection compliance

The Marketing Manager is WAL's appointed compliance officer in respect of its data protection activities.