

World Jungle GDPR and Data Protection Policy

Updated: August 2025

Review date: August 2026

Contents

1. The Basics
2. Guidelines for Staff
3. Company Policy

1. The Basics

Data Protection is important, not because it is about protecting data, but because it is about protecting people. People can be harmed if their data is misused or if it gets into the wrong hands through poor security or through careless disclosures. They can be harmed if their data is inaccurate or insufficient and decisions are made about them, or about what services to provide them with.

Being unclear about Data Protection also runs the risk that people misunderstand it and possibly over-react, becoming obstructive when there is no need to be, causing hassle for individuals and other organisations.

If you harm someone through a breach of Data Protection, your organisation may well have to pay them compensation. But it's not really about protecting the organisation from financial harm; it's about making sure that everyone in the organisation is able to treat people properly because they know what they are supposed to do.

The Data Protection Act of 2018 has at its heart the principle that confidential information about all of us must be protected. The Act covers manual records and computerised records and will apply to virtually all personnel and employment files and to any kind of database which contains customer or client information.

It is about the **processing** of data and processing covers:

- . Collecting data
- . Holding on to that data
- . Gaining access to it
- . Using it
- . Disclosing it
- . Destroying it

Firstly, it states that everyone responsible for using personal data has to follow strict rules called 'data protection principles'. They must make sure the information is:

- used fairly, lawfully and transparently
- used for specified, explicit purposes
- used in a way that is adequate, relevant and limited to only what is necessary
- accurate and, where necessary, kept up to date
- kept for no longer than is necessary
- handled in a way that ensures appropriate security, including protection against unlawful or unauthorised processing, access, loss, destruction or damage

The second area covered by the Act provides individuals with important rights, including the right to find out what personal information is held on computer and most paper records. The Act also provides the individual with the right to erasure.

Should an individual or organisation feel they've been denied access to personal information which they are entitled to or feel their information has not been handled according to the eight principles, they can contact the Information Commissioner's Office for help. Complaints are usually dealt with informally, but if this isn't possible, enforcement action can be taken.

Company Policy

World Jungle has to collect and use certain types of information about its employees, customers, and other individuals who come into contact with the Company.

The purpose of the Policy is to enable the Company to:

- Comply with the law in respect of the data which it holds about individuals
- Follow good practice
- Protect our customers, staff and other individuals
- Protect the organisation from the consequences of a breach of its responsibilities

The Company commits to:

- Complying with both the law and good practice
- Respecting the rights of individuals
- Being open and honest with individuals whose data is held

- Providing training and support for staff who handle personal data, so that they can act confidently and consistently

The company recognises that its first priority under the Data Protection Act is to avoid causing harm to individuals. In the main this means:

- Keeping information securely in the right hands, and
- Holding good quality information

The company recognises that these are the key areas of risk and this policy is designed to address these.

In addition to being open and transparent, the Company will seek to give individuals as much choice as is possible and reasonable over what data is held and how it is used.

Via appropriate management and strict application of criteria and controls, the Company will:

1. Observe fully conditions regarding the fair collection and use of information
2. Meet its legal obligations to specify the purposes for which information is used
3. Collect and process appropriate information and only to the extent that it is needed to fulfil operational needs or to comply with any legal requirements
4. Ensure the quality of information used
5. Apply strict checks to determine the length of time information is held
6. Ensure that the rights of people about whom information is held can be fully exercised under the Act. (These include: the right to be informed that processing is being undertaken, the right of access to one's personal information, the right to prevent processing in certain circumstances and the right to correct, rectify, block or erase information).
7. Take appropriate technical and organisational security measures to safeguard personal information
8. Ensure that personal information is not transferred abroad without suitable safeguards
9. Treat people justly and fairly whatever their age, religion, gender, disability, sexual orientation or ethnicity when dealing with requests for information
10. Set clear procedures for responding to requests for information

Additionally, the Company will ensure that:

1. Everyone managing and handling personal information understands that they are contractually responsible for following good data Protection Practice
2. Everyone managing and handling personal information is appropriately trained to do so
3. Everyone managing and handling personal information is appropriately supervised
4. Anybody wanting to make enquiries about handling personal information knows what to do
5. Queries about handling personal information are promptly and courteously dealt with
6. Methods of handling personal information are clearly described
7. A regular review and audit is made of the way personal information is held, managed and used
8. Methods of handling personal information are regularly assessed and evaluated
9. A breach of the rules and procedures identified in this policy by a member of staff may lead to disciplinary action being taken

This policy will be updated as necessary to reflect best practice in data management, security and control and to ensure compliance with any changes or amendments made to the Data Protection Act 2018.

Responsibilities

The Data Protection officer for the company is its Co Director **Jane Manning**. She is the Data Controller as defined by the Information Commissioner's office. The Data Controller's responsibilities include:

- Ensuring that the organisation complies with its legal obligations and with changes in the law as they may occur
- Reviewing Data Protection in the company and related policies
- Advising members of staff on Data Protection issues
- Ensuring that Data Protection induction and training takes place

- Handling subject access requests
- Approving Unusual or controversial disclosures of personal data

In each department where personal data is handled, the department manager is responsible for ensuring that the operational procedures including induction and training, comply with the Company's requirements for Data Protection and its stated policy.

All staff (and volunteers) are required to read and understand and accept any policy and procedure that relates to the personal data they may handle in the course of their work.

Significant breaches of the Company's policy will be handled under the standard disciplinary procedures.

Confidentiality

See separate document 'Confidentiality Policy'

Security

Not to be confused with confidentiality, this section of the policy only addresses security issues relating to personal data. It does not cover security of the building, business-continuity or any other aspect of security.

The security of personal data can be at risk in certain circumstances and it is very important that all staff recognise what these could be. For example, the Company has identified the following risks:

- Information passing between sites could go astray or be misdirected
- Staff with access to personal information could misuse it
- Poor website security might give a means of access to information about individuals if individual details are made accessible online.
- Staff may be tricked into giving away information, either about customers or colleagues, through 'social engineering'. For example, inappropriately giving out staff details over the telephone.

1. Staff must ensure that access to their computer' including laptops is password protected and that password is only known to that staff member and to the network administrator

2. Memory sticks, CDs or writable media must be secured in a locked environment

3. Back up procedures are carried out by the administration team at the end of every working day

4. All staff should aim to adopt a 'clear desk policy.' Personal data, for example, learner files, must not be left unsecured overnight and should not be left during the day in a position which could allow unauthorised access

5. No data of any kind should ever be left unattended allowing access to visitors or other unauthorised people

6. No access by visitors or other unauthorised people should ever be granted to the company's computerised systems

Data Recording and Storage

The company will regularly review its procedures for ensuring that its records remain accurate and consistent and, in particular:

- ICT systems are designed, as far as is possible, to encourage and facilitate the entry of accurate data
- Data on any individual will be held in as few places as necessary and all staff will be discouraged from establishing unnecessary additional data sets
- Effective procedures are in place so that all relevant systems are updated when information about any individual changes
- Staff who keep more detailed information about individuals will be given additional guidance on accuracy in record keeping
- Manually maintained learner data and employer (client) data is stored in the locked central filing area only and is regularly archived (six monthly)
- Archived paper records are stored off site and as different categories of data reach the end of their retention period, these are collected and taken away for destruction by an accredited organisation

Transparency

The company is committed to ensuring that in principle Data subjects are aware that their data is being process and:

- For what purpose it is being processed
- What types of disclosure are likely
- How to exercise their rights in relation to the data

Data Subjects will generally be informed in the following ways:

- Staff - via the induction process and induction pack
- Others – via initial notice, consent forms, etc.

Consent

Under the Data Protection Act 2018 and GDPR, consent is one of the grounds for lawfully processing data (other grounds include, by contract, by legal obligation, by vital interest, by public task, and by legitimate interest). When information is collected we will be clear about what elements are optional.

Consent must be freely given, specific, informed and unambiguous.

Consent can be withdrawn at any point.

GDPR

Scope

This policy applies to all personal data processed by World Jungle and is part of World Jungle's approach to compliance with data protection law. All World Jungle staff are expected to comply with this policy and failure to comply may lead to disciplinary action for misconduct, including dismissal.

Data protection principles

World Jungle complies with the data protection principles set out below. When processing personal data, it ensures that:

- it is processed lawfully, fairly and in a transparent manner in relation to the data subject ('lawfulness, fairness and transparency')
- it is collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes ('purpose limitation')
- it is all adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed ('data minimisation')
- it is all accurate and, where necessary, kept up to date and that reasonable steps will be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay ('accuracy')
- it is kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed ('storage limitation')

- it is processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures ('integrity and confidentiality')

World Jungle will facilitate any request from a data subject who wishes to exercise their rights under data protection law as appropriate, always communicating in a concise, transparent, intelligible and easily accessible form and without undue delay.

Process/procedures/guidance

World Jungle will:

- ensure that the legal basis for processing personal data is identified in advance and that all processing complies with the law
- not do anything with your data that you would not expect given the content of this policy and the fair processing or privacy notice
- ensure that appropriate privacy notices are in place advising staff and others how and why their data is being processed, and, in particular, advising data subjects of their rights
- only collect and process the personal data that it needs for purposes it has identified in advance
- ensure that, as far as possible, the personal data it holds is accurate, or a system is in place for ensuring that it is kept up to date as far as possible
- only hold onto your personal data for as long as it is needed, after which time World Jungle will securely erase or delete the personal data – World Jungle's data retention policy sets out the appropriate period of time
- ensure that appropriate security measures are in place to ensure that personal data can only be accessed by those who need to access it and that it is held and transferred securely

World Jungle will ensure that all staff who handle personal data on its behalf are aware of their responsibilities under this policy and other relevant data protection and information security policies, and that they are adequately trained and supervised.

Breaching this policy may result in disciplinary action for misconduct, including dismissal. Obtaining (including accessing) or disclosing personal

data in breach of World Jungle's data protection policies may also be a criminal offence.

Data Subject Rights

World Jungle has processes in place to ensure that it can facilitate any request made by an individual to exercise their rights under data protection law. All staff have received training and are aware of the rights of data subjects. Staff can identify such a request and know who to send it to.

All requests will be considered without undue delay and within one month of receipt as far as possible.

Subject access: the right to request information about how personal data is being processed, including whether personal data is being processed and the right to be allowed access to that data and to be provided with a copy of that data along with the right to obtain the following information:

- the purpose of the processing
- the categories of personal data
- the recipients to whom data has been disclosed or which will be disclosed
- the retention period
- the right to lodge a complaint with the Information Commissioner's Office
- the source of the information if not collected direct from the subject, and
- the existence of any automated decision making

Rectification: the right to allow a data subject to rectify inaccurate personal data concerning them.

Erasure: the right to have data erased and to have confirmation of erasure, but only where:

- the data is no longer necessary in relation to the purpose for which it was collected, or
- where consent is withdrawn, or
- where there is no legal basis for the processing, or
- there is a legal obligation to delete data

Restriction of processing: the right to ask for certain processing to be restricted in the following circumstances:

- if the accuracy of the personal data is being contested, or
- if our processing is unlawful but the data subject does not want it erased, or
- if the data is no longer needed for the purpose of the processing but it is required by the data subject for the establishment, exercise or defence of legal claims, or
- if the data subject has objected to the processing, pending verification of that objection

Data portability: the right to receive a copy of personal data which has been provided by the data subject and which is processed by automated means in a format which will allow the individual to transfer the data to another data controller. This would only apply if World Jungle was processing the data using consent or on the basis of a contract.

Object to processing: the right to object to the processing of personal data relying on the legitimate interests processing condition unless World Jungle can demonstrate compelling legitimate grounds for the processing which override the interests of the data subject or for the establishment, exercise or defence of legal claims.

Special category personal data

This includes the following personal data revealing:

- racial or ethnic origin
- political opinions
- religious or philosophical beliefs
- trade union membership
- the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person
- an individual's health
- a natural person's sex life or sexual orientation
- criminal convictions or offences

World Jungle processes special category data of clients and third parties as is necessary to provide legal services for the establishment, exercise or defence of legal claims.

World Jungle processes special category data of employees as is necessary to comply with employment and social security law. This policy sets out the safeguards we believe are appropriate to ensure that we comply with the

data protection principles set out above. World Jungle also has a data retention policy which sets out how long special category data will be held onto.

Responsibility for the processing of personal data

The partners of World Jungle take ultimate responsibility for data protection.

If you have any concerns or wish to exercise any of your rights under the GDPR, then you can contact the data protection lead in the following ways:

Name. Ben Ward

Address Dursley Library, May Lane, Dursley Glos

Email Ben@worldjungle.org.uk

Telephone 07889 512644

Monitoring and review

This policy was last updated in August 2025 and shall be regularly monitored and reviewed, at least every two years.