DATA PROTECTION AND GDPR POLICY

WONDERLAND
COMMUNICATIONS

OVERVIEW

The Company take the security and privacy of your data seriously. We need to gather and use information or 'data' about you as part of our business and to manage our relationship with you. 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, workers, volunteers, apprentices and consultants. If you fall into one of these categories, then you are a 'data subject' for the purposes of this policy. You should read this policy alongside your contract of employment (or contract for services) and any other notice we issue to you from time to time in relation to your data.

The Company has measures in place to protect the security of your data and details can be obtained from a Director of the business.

We will only hold data for as long as necessary for the purposes for which we collected it and we adhere to retention guidelines policy (details of which can be obtained from a Director of the business).

The Company is a 'data controller' for the purposes of your personal data. This means that we determine the purpose and means of the processing of your personal data.

This policy explains:

- how Wonderland will hold and process your information
- your rights as a data subject
- your obligations when obtaining, handling, processing or storing personal data in the course of working for, or on behalf of, the Company

This policy does not form part of your contract of employment (or contract for services if relevant) and can be amended by the Company at any time.

It 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 Company intends to comply with the 2018 Act and the GDPR.

DATA PROTECTION PRINCIPLES

Personal data must be processed in accordance with six 'Data Protection Principles.' It must:

a. be processed fairly, lawfully and transparently;

b. be collected and processed only for specified, explicit and legitimate purposes;

c. be adequate, relevant and limited to what is necessary for the purposes for which it is processed;

d. be accurate and kept up to date. Any inaccurate data must be deleted or rectified without delay;

e. not be kept for longer than is necessary for the purposes for which it is processed; and

f. be processed securely.

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

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, your doctor, 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 a Director or other colleagues.

- We will collect and use the following types of personal data about you:

    a) recruitment information such as your application form and CV, references, qualifications and membership of any professional bodies and details of any pre-employment assessments;

    b) your contact details and date of birth;

    c) the contact details for your emergency contacts;

    d) information about your contract of employment (or services) including start and end dates of employment, role and location, working hours, details of promotion, salary (including details of previous remuneration), pension, benefits and holiday entitlement;

    e) your bank details and information in relation to your tax status including your national insurance number;

    f) your identification documents including passport and driving licence and information in relation to your immigration status and right to work for us;

g) information relating to disciplinary or grievance investigations and proceedings involving you (whether or not you were the main subject of those proceedings);

h) information relating to your performance and behaviour at work;

i) training records;

j) electronic information in relation to your use of IT systems/swipe cards/telephone systems;

k) your images (whether captured on CCTV, by photograph or video); and

l) any other category of personal data which we may notify you of from time to time.

HOW WE DEFINE SPECIAL CATEGORIES OF PERSONAL DATA

'Special categories of personal data' are types of personal data consisting of information as to:

a. your racial or ethnic origin;

b. your political opinions;

c. your religious or philosophical beliefs;

d. your trade union membership;

e. your genetic or biometric data;

f. your health;

g. your sex life and sexual orientation; and

h. any criminal convictions and offences.

We may hold and use any of these special categories of your personal data in accordance with the law.

You may be thinking, "why on earth would Wonderland hold info about people's race, political opinions, sex life, sexual orientation or religious beliefs? That's weird / outrageous".

We wanted to make sure you knew the answer to this…

We're not just being nosey, and we might not intentionally hold such info (in the sense that we don't do any diversity monitoring), BUT we - the team - emailing each other, writing things in emails or whatever about our own / others' beliefs count as "processing data".

As we (Wonderland) are the data processor, we (Wonderland) are liable.

The definition of "Special categories of personal data" is a legal definition and this policy details what we can and can't do with that data.

HOW WE DEFINE PROCESSING

'Processing' means any operation which is performed on personal data such as:

a. collection, recording, organisation, structuring or storage;

b. adaption or alteration;

c. retrieval, consultation or use;

d. disclosure by transmission, dissemination or otherwise making available;

e. alignment or combination; and

f. restriction, destruction or erasure.

This includes processing personal data which forms part of a filing system and any automated processing.

HOW WILL. WE PROCESS YOUR PERSONAL DATA?

The Company 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:

a) performing the contract of employment (or services) between us;

b) complying with any legal obligation; or

c) if it is necessary for our legitimate interests (or for the legitimate interests of someone else). However, we can only do this if your interests and rights do not override ours (or theirs). You have the right to challenge our legitimate interests and request that we stop this processing. See details of your rights below.

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.

If you choose not to provide us with certain personal data, you should be aware that we may not be able to carry out certain parts of the contract between us.

For example, if you do not provide us with your bank account details, we may not be able to pay you.

It might also stop us from complying with certain legal obligations and duties which we have such as to pay the right amount of tax to HMRC or to make reasonable adjustments in relation to any disability you may suffer from.

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 (and see section below for the meaning of the asterisks):

a. to decide whether to employ (or engage) you;

b. to decide the terms of your contract with us;

c. to check you have the legal right to work for us;

d. to carry out the contract between us including where relevant, its termination;

e. training you and reviewing your performance*;

f. to decide whether to promote you;

g. to decide whether and how to manage your performance, absence or conduct*;

h. to carry out a disciplinary or grievance investigation or procedure in relation to you or someone else;

i. to determine whether we need to make reasonable adjustments to your workplace or role because of your disability*;

j. to monitor diversity and equal opportunities*;

k. to monitor and protect the security (including network security) of the Company, of you, our other staff, clients and others;

l. to monitor and protect the health and safety of you, our other staff, clients and third parties*;

m. to pay you and provide pension and other benefits in accordance with the contract between us*;

n. paying tax and national insurance;

o. to provide a reference upon request from another employer;

p. to pay trade union subscriptions*;

q. monitoring compliance by you, us and others with our policies and our contractual obligations*;

r. to comply with employment law, immigration law, health and safety law, tax law and other laws which affect us*;

s. to answer questions from insurers in respect of any insurance policies which relate to you*;

t. running our business and planning for the future;

u. the prevention and detection of fraud or other criminal offences;

v. to defend the Company in respect of any investigation or litigation and to comply with any court or tribunal orders for disclosure*; and

w. for any other reason which we may notify you of from time to time.

We will only process special categories of your personal data (see above) in certain situations in accordance with the law. For example, we can do so if we have your explicit consent. If we asked for your consent to process a special category of personal data, then we would explain the reasons for our request. You do not need to consent and can withdraw consent later if you choose by contacting a Director of the business.

We do not need your consent to process special categories of your personal data when we are processing it for the following purposes, which we may do:

a. where it is necessary for carrying out rights and obligations under employment law;
b. where it is necessary to protect your vital interests or those of another person where you/they are physically or legally incapable of giving consent;
c. where you have made the data public;
d. where processing is necessary for the establishment, exercise or defence of legal claims; and
e. where processing is necessary for the purposes of occupational medicine or for the assessment of your working capacity.

We might process special categories of your personal data for the purposes in the paragraph above which have an asterisk beside them. In particular, we will use information in relation to:

a. your race, ethnic origin, religion, sexual orientation or gender to monitor equal opportunities;
b. 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; and
c. your trade union membership to pay any subscriptions and to comply with our legal obligations in respect of trade union members.
d. your background and criminal record history to comply with any legal obligations

We do not take automated decisions about you using your personal data or use profiling in relation to you.

SHARING YOUR PERSONAL DATA

Sometimes we might share your personal data with our contractors, partners, advisers and agents to carry out our obligations under our contract with you or for our legitimate interests. This enables us to process payroll and to manage our relationship with you.

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.

We do not send your personal data outside the European Economic Area. If this changes you will be notified of this and the protections which are in place to protect the security of your data will be explained.

HOW SHOULD YOU PROCESS COMPANY PERSONAL DATA FOR THE COMPANY?

Everyone who works for, or on behalf of, the Company has some responsibility for ensuring data is collected, stored and handled appropriately, in line with this policy:

- The Company's Data Protection Manager (Jamie) is responsible for reviewing this policy and any risks in relation to the processing of data. You should direct any questions in relation to this policy or data protection to this person.
- You should only access personal data covered by this policy if you need it for the work you do for, or on behalf of the Company and only if you are authorised to do so. You should only use the data for the specified lawful purpose for which it was obtained.
- You should 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 Manager.
- You should lock drawers and filing cabinets. Do not leave paper with personal data lying about.
- You should not take personal data away from the Company's premises without authorisation from your line manager or the Data Protection Manager.
- Personal data should be shredded and disposed of securely when you have finished with it.
- You should ask for help from our Data Protection Manager 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 in accordance with our disciplinary procedure.

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

HOW SHOULD YOU PROCESS CLIENT AND JOURNALIST DATA FOR THE COMPANY?

Everyone who works for, or on behalf of, the Company has responsibility for ensuring client and journalist data (aka the data that we access on a daily basis to fulfil our roles) is collected, stored and handled appropriately, in line with this policy:

- Along with all the above points:

- The day to day obtaining of journalist data from the Gorkana media database is covered by our contract with Gorkana who are covered by the GDPR.

- On the occasion where it is required to request home addresses from a journalist, this should be requested per campaign, obtaining consent from the journalist, with no data kept on record thereafter. All data (including emails containing personal details and addresses) should be deleted within 48 hours of PCA/campaign completion.

- Any requests from journalists to be removed from your media lists should be adhered to. A list of all those journalists who have asked to opt out from receiving emails/we shouldn't be sending emails to, can be found here. Please make sure to have a look over pre-correspondence with journalists.

- Similarly, in relation to occasions where client and consumer data is requested (e.g., for mailer or competition winners), data should be encrypted before being transferred electronically to authorised external contacts, and then deleted within 48 hours of campaign completion.

HOW TO DEAL WITH DATA BREACHES

We have robust 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 Data Protection Manager immediately and keep any evidence you have in relation to the breach.

SUBJECT ACCESS REQUESTS

Data subjects can make a 'subject access request' ('SAR') to find out the information we hold about them. This request must be made in writing. If you receive such a request, you should forward it immediately to the Data Protection Manager who will coordinate a response.

If you would like to make a SAR in relation to your own personal data, you should make this in writing to the Data Protection Manager. We must respond within one month unless the request is complex or numerous in which case the period in which we must respond can be extended by a further two months.

There is no fee for making a SAR.

However, if your request is manifestly unfounded or excessive, we may charge a reasonable administrative fee or refuse to respond to your request.

YOUR DATA SUBJECT RIGHTS

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

2. You have the right to access your own personal data by way of a subject access request (see above).

3. You can correct any inaccuracies in your personal data. To do you should contact the Data Protection Manager.

4. 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. To do so you should contact the Data Protection Manager.

5. While you are requesting that your personal data is corrected or erased or are contesting the lawfulness of our processing, you can apply for its use to be restricted while the application is made. To do so you should contact the Data Protection Manager.

6. 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.

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

8. You have the right to receive a copy of your personal data and to transfer your personal data to another data controller. We will not charge for this and will in most cases aim to do this within one month.

9. With some exceptions, you have the right not to be subjected to automated decision-making.

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

11. In most situations we will not rely on your consent as a lawful ground to process your data. If we do however request your consent to the processing of your personal data for a specific purpose, you have the right not to consent or to withdraw your consent later. To withdraw your consent, you should contact the Data Protection Manager.

12. 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.