Data Protection Policy	Version:	2.1
	Status:	Final
	Date:	8/1/21

1. Approval Record

Name	Role	Date
Rebecca Clake	Office and HR Lead	1/8/20
Tonino Ciuffini	Data Protection Officer	1/8/20

2. Version History

Version	Date	Author	Description (nature of change/update)
0.1	1/6/20	Rebecca Clake	Initial Creation – Document design
2.0	1/8/20	Rebecca Clake	Final version
2.1	8/1/21	Rebecca Clake	Annual review and version control update

3. Related Documents

Document Title	Location	Version Number
IT Security and Social Media Policy	HR System	V2.1
Records Management Policy	HR System	V1.1

4. Review and Distribution List

Name	Role	Review Required
Tonino Ciuffini	Data Risk Officer	Contributor / Reviewer
Rebecca Clake	Office and HR Lead	Contributor / Reviewer
All Staff		For Information Only

5. Regulatory Requirements

Data Protection Act, General Data Protection Regulations

6. Introduction

6.1 Purpose

This policy sets a framework for handling data on behalf of We are Digital. The policy ensures members of staff act reasonably when handling any data or accessing systems containing personal data.

6.2 Scope

This policy applies to all members of staff who work under a contract of employment with We are Digital. It also applies to agency staff, contractors, and others employed under a contract of service.

7. Roles and Responsibilities

RACI	Role	Role Holder(s)	Key Responsibilities
Responsible	Process SME	Tonino Ciuffini	• Ensuring process document accurately reflects current practice • Contributing to process changes and improvements, as and when identified
Accountable	Process Owner	Tonino Ciuffini	• Overall ownership and accountability for process definition and execution • Leading change for improving the process • Approval point for any changes/update to the process definition • Ensuring that any changes are properly documented and communicated • Ensuring that ongoing monitoring is in place and carried out
Consulted	Head of People	Rebecca Clake	• Monitoring adherence to agreed process through periodic quality reviews
Informed	All Staff Subcontractors		• Read and accept of document must be completed in HR system • To be included in subcontractor paperwork

8. Instruction

The security and privacy of your data is taken seriously by us but we need to gather and use information or 'data' about you as part of our business and to manage our relationship with you. We are committed to complying with our all the Data Protection legal obligations.

This policy applies to current and former employees, workers, volunteers, interns, 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 separate policies and privacy notices in place in respect of job applicants, customers, suppliers and other categories of data subject. A copy of these can be obtained from the person responsible for Data in the Company.

The Company has taken steps to protect the security of your data in accordance with our Data Security Policy and will train employees about their data protection responsibilities as part of the induction process. We will only hold data for as long as necessary for the purposes for which we collected it.

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 the Company will hold and process your information. It explains your rights as a data subject. It also explains 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.

8.1 Data Protection Principles

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

- be processed fairly, lawfully and transparently
- be collected and processed only for specified, explicit and legitimate purposes
- be adequate, relevant and limited to what is necessary for the purposes for which it is processed
- be accurate and kept up to date. Any inaccurate data must be deleted or rectified without delay
- not be kept for longer than is necessary for the purposes for which it is processed
- be processed securely

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

8.2 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 your manager or other colleagues.

The types of personal data we collect and use about you is included in the Privacy Notice that is issued with your contract of employment.

8.3 How we Define Special Categories of Personal Data

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

- your racial or ethnic origin
- your political opinions
- your religious or philosophical beliefs
- your trade union membership
- your genetic or biometric data
- your health
- your sex life and sexual orientation
- any criminal convictions and offences

We may hold and use any of these special categories of your personal data, as detailed in the Privacy Notice, in accordance with the law.

8.4 How we Define Processing

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

- collection, recording, organisation, structuring or storage
- adaption or alteration
- retrieval, consultation or use
- disclosure by transmission, dissemination or otherwise making available
- alignment or combination
- restriction, destruction or erasure

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

8.5 How will we Process your Personal Data

The Company will process your personal data (including special categories of personal data). We will use your personal data for:

- performing the contract of employment (or services) between us
- complying with any legal obligation
- 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.

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.

Examples of when we might process your personal data can be found in the Privacy Notice. We will only process special categories of your personal data 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 the person responsible for Data in the Company.

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:

- where it is necessary for carrying out rights and obligations under employment law
- 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
- where you have made the data public
- where processing is necessary for the establishment, exercise or defence of legal claims
- where processing is necessary for the purposes of occupational medicine or for the assessment of your working capacity
- where it is necessary for the purposes of criminal records checks (DBS check) in order for you to fulfil the requirements of your role

We might process special categories of your personal data for the purposes stated in the Privacy Notice, in particular, we may use information in relation to:

- your race, ethnic origin, religion, sexual orientation or gender to monitor equal opportunities
- 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
- your trade union membership to pay any subscriptions and to comply with our legal obligations in respect of trade union members
- your criminal record history to comply with our obligations in relation to your role

8.6 Sharing your Personal Data

Sometimes we might share your personal data with group companies or our business partners, contractors and agents to carry out our obligations under our contract with you or for our legitimate interests.

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 use the following contractors to carry out our Company business:

- Outsourced HR company

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.

8.7 How Should you Process 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 and the Company's IT Security and Data Retention policies.

The Data Risk Officer is responsible for reviewing this policy on the Company's data protection responsibilities 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 and address any written requests to them.

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

- 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 person responsible for Data in your Company
- You should lock drawers and filing cabinets. Do not leave paper with personal data lying about
- You should not take personal data away from Company's premises without authorisation from your line manager or of the person responsible for Data in your Company
- Personal data should be shredded and disposed of securely when you have finished with it
- You should ask for help from the person responsible for Data in your Company 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

8.8 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 person responsible for Data immediately and keep any evidence you have in relation to the breach.

8.9 Subject Access Request

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 the person responsible for Data in your Company 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 person responsible for Data in the Company. 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.

8.10 Your Data Subject Rights

- You have the right to information about what personal data we process, how and on what basis as set out in this policy
- You have the right to access your own personal data by way of a subject access request (see above)

- You can correct any inaccuracies in your personal data. To do you should contact of the person responsible for Data in the Company
- 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 person responsible for Data in the Company
- 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 person responsible for Data in the Company
- 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
- You have the right to object if we process your personal data for the purposes of direct marketing
- 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
- With some exceptions, you have the right not to be subjected to automated decision-making
- You have the right to be notified of a data security breach concerning your personal data
- 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 person responsible for Data in the Company

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.

9. Quality Control Log

No	Risk/Issue	Control	Control in Place Y/N
1	Reliance on key individuals (single point of failure)	Manual checks by another person – segregation of duties	Y

10. Glossary

Term	Description
SAR	Subject access request
ICO	Information Commissioner Office