Data Protection Policy for Employees & Freelancers

1. Preface

1.1 Document Owner

Name	Job title
Jacqueline Moreton	Chief Privacy Officer/ General Council

1.2 Approved By

Name	Job Title
Jacqueline Moreton	Chief Privacy Officer

1.3 Data Classification Label

Highly Sensitive	☐
Sensitive	☐
Internal	☐
Public	☒

1.4 Change History

Version	Date	Revision Description	Changed By
1.0	Feb 2017	Initial Draft	Tracey Spevack
2.0	Mar 2018	Revised draft for GDPR compliance	Gregory Stoneham
3.0	Oct 2018	Changed to 'Fremantle'	Gregory Stoneham

2. Glossary of Terms

Fremantle Group Members	Fremantlemedia Group Limited, any of its subsidiaries and any subsidiaries of RTL Group SA managed as part of the Fremantle group of companies.
Fremantle Staff	Any persons employed or engaged by or on behalf of Fremantle, whether permanent or temporary employees, contractors (including freelancers) or consultants.
Chief Privacy Officer	Person ultimately responsible for privacy and data protection at Fremantle
Data Protection Coordinator (DPC)	The designated person (or persons) in Fremantle Group Members responsible for compliance with data protection laws and this policy within their respective business unit.
Personal Data	Any Data relating to a Data Subject, such as name, date of birth, identification number, location data or address, online identifier or one or more factors specific to their physical, physiological, genetic, mental, economic, cultural, social or economic, identity of that person.
Sensitive Personal Data	Personal Data that reveals a Data Subject's racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership(s), genetic or biometric data, sexual orientation, sex life details, or data concerning mental or physical health.
Child's Personal Data	Any Personal Data (including Sensitive Personal Data) relating to a Data Subject under the age of 13.
Data Sharing Agreement	A contract or part of a contract regulating how organisations and/or individuals share data within the corporate group or with third parties.
Data Controller	A Data Controller determines the purposes for which and the manner in which any personal data are, or are to be, processed.
Data Processor	A Data Processor is responsible for processing personal data on behalf of a Data Controller.
Data Sub-Processor	A sub-processor (or "level 2 processor") is responsible for processing personal data on behalf of and when engaged by a Data Processor as defined by Article 28(2) and (4) of the GDPR.
Data Subject Access	The right of a data subject to access their own personal data as defined by GDPR Articles 12 and 15 and as interpreted in Fremantle's **Subject Access Request Response Policy**.
European Economic Area (EEA)	Members states of the European Union and the member states of the European Free Trade Association.

3. Introduction

The Data Protection Act 2018 ("the Act") sets out the principles that the Company must follow when processing personal data about individuals, and also gives individuals certain rights in relation to personal data that is held about them. This Policy aims to:

- assist the Company in meeting its obligations under the Act;
- regulate the Company's use of personal data relating to employees and others who work for the Company; and
- ensure that employees and others working for the Company are aware of both their rights in relation to the personal data that the Company holds about them, and their responsibilities as regards personal data it may hold about other individuals working for the Company.

For ease of reference, this Policy refers to "employees", but it applies equally to individuals working for the Company in other capacities such as freelancers, contractors, and agency workers, where the Company holds data relating to them. The Company's policies are explained in detail in Privacy and Data Protection Policy and the Data Retention Policy.

4. Data Protection Principles

The Act places an obligation on "data controllers", such as the Company, to observe six data protection principles. In summary these are that personal data must be:

- processed fairly and lawfully;
- Data should be collected for specified, explicit and legitimate purposes
- Processing of personal data must be adequate, relevant and limited to what is necessary
- accurate and, where necessary, kept up to date
- kept for no longer than is necessary;
- kept secure;

All employees also have an obligation to comply with these principles where necessary. Please refer to Section 7 of this Policy for further guidance.

5. What is Personal Data and Processing?

Personal data includes information which relates to or identifies a living individual. The data protection principles apply to personal data which is either automatically processed (e.g. on a database) or which is held in a highly structured filing system which falls within the Act.

There are also special categories of personal data that are more sensitive ("sensitive data"). Personal data is sensitive if it relates to matters such as race,ethnic origin, political opinions, trade union membership, health, genetic data, biometric data, sexual orientation and sex life or any criminal offence or related proceedings. Section 5.3 of this Policy explains the types of information the Company tends to hold which amounts to sensitive personal data.

"Processing" is the term used in the Act to refer to a wide range of activities in relation to personal data including its collection, retention, use, disclosure, and final destruction or erasure.

6. The Company's Obligations

One of the ways in which the Company can take steps to comply with its obligations under the data protection principles is through legitimate interests and/or meeting contractual obligations between the Company and Employees when processing employment related personal data. This is not the only way that the Company can comply with its obligations under the Act and that the Company will still need to process certain personal data, sensitive data, or to transfer it to other group companies in a given situation for the purposes of its legal obligations (for example Social Security) and the purposes set out in this Policy. You will not be subjected to any detriment if you object to the processing of specific types of data although there may be certain consequences which will be explained to you.

The Company has appropriate safeguards in place to ensure compliance with the data protection principles.

7. What types of Personal Data does the Company hold?

7.1 General Employee Information

The Company holds and processes certain data about you as part of its general employee records. Its records include:

- name, address, phone numbers, and other contact details;
- date of birth, NI number and marital/civil partnership status;
- CVs, application forms, details of education, job history and experience (both within the Company and previously), qualifications, contracts of employment, offer letters and references;
- Copy of passport and other documents showing immigration status;
- emergency contact details;
- full details of current and previous positions within the Company, details of compensation and benefits (including details of Company loans and pension contributions),
- records relating to holiday and other leave;
- details of development needs and achievements, records and documentation relating to any appraisals, performance reviews, disciplinary matters concerning you or in relation to which you have been involved, or grievances you have raised or which have been raised by others about you;
- details of nominated beneficiaries for the purposes of the pension and life assurance schemes;
- details of dependants for the purpose of administering benefits such as childcare vouchers and private medical/dental insurance.
- Driving licence in order to comply with our health and safety obligations for those who drive for work.

Our systems will also collect and retain personal data; these might include our IT system, entry passes or tapes from CCTV cameras**.**

Obviously, it is not possible to list every type of information which may be held by the Company about every employee in this document. This list only contains examples of

the usual types of general employee information the Company holds and is not exhaustive. Much of this information will amount to personal data for the purposes of the Act depending on the context in which it is held by us.

7.2 Purpose of Processing General Employee Information

The Company needs to collect and use personal data about employees for a variety of personnel, administration, employee, work and general business management purposes. These include administration of the payroll system, the administration of employee benefits (such as bonuses, pensions, leave entitlements), verifying an employee's right to work in the UK, facilitating the management of work and employees, carrying out appraisals, performance reviews and salary reviews, disciplinary investigations and meetings, checking employees' driving licences to operate and check compliance with the Company's employment rules and policies, to operate the Company's IT and communications systems such as the use of mobile phones, ipads and laptops, and to check for unauthorised use of those systems (including, where appropriate, monitoring), and to comply with record keeping and other legal obligations including its obligations under the Data Protection Act 2018.

7.3 Sensitive Personal Data

As noted in Section 3 of this Policy the Act also recognises special categories of information known as sensitive personal data. The only information which the Company collects and processes which may amount to sensitive personal data is information relating to your health, race or ethnic origin.

7.4 Health Information

The particular information that the Company presently holds relating to your health is records of sickness absence and medical certificates (including the Company's Self-Certified Sickness Form) and any medical reports which you have provided or have been obtained by the Company with your prior consent.

The purpose of obtaining and keeping this sort of information is to assess eligibility for or administer and pay benefits related to ill-health such as Company and statutory sick pay, private medical insurance, group income protection insurance and life insurance.

We may also use any medical reports we have obtained in order to assess or determine your fitness for employment, continued employment or a particular role or task, or to assess any risk to your health. The Company also needs this information to monitor and manage sickness absence, and to comply with obligations under Health and Safety legislation, including its obligations to protect your health and safety at work and the health and safety of others, and the Equality Act 2010.

These obligations mean that from time to time the Company may need to obtain and retain certain material relating to your health in order to assess your suitability to carry out your role or certain aspects of your role, or for an alternative role, or to assess issues over your performance.

The records contained are kept securely by the Company and are subject to access controls. Those who may have access to such records include HR and managers may have occasional access to specific relevant information to enable them to exercise their management responsibilities.

Where employees object to the collection, use, or retention of health information they will not be subjected to any detriment although there may be certain consequences which will be discussed with you. Examples include the Company's inability to progress an application for a particular benefit or its need to make a business decision based on information available to it.

7.5 Race, Ethnic Origin etc.

The Company may hold information relating to your race or ethnic origin where this has been provided on an equal opportunities monitoring form. The purpose of keeping this sort of information is to monitor the effectiveness of the Company's Diversity Policy.

7.6 Information Relating to the Use of IT Systems

The Company processes personal data relating to employees as part of its IT and communications systems.

The Company's policy as regards the use of these systems by employees and others is explained in detail in the Company's Acceptable Use Policy. This also explains the Company's policy on monitoring.

8. Keeping Personal Data

8.1 Payroll & Pensions Databases

Some of the employee information described in Section 5 is stored on HR databases for payroll and pension purposes. The databases are controlled by the Company's payroll providers and pension administrators and the Company's Human Resources Department in London. The database can be accessed electronically by the Company's Human Resources staff in London.

There are security measures in place, including the use of passwords, and other access controls which will ensure the confidentiality of the information contained in the database and these measures will be reviewed over time and upgraded in line with legal and technological developments.

8.2 Personnel Files

The remainder of the employee information described in Section 5 is kept in the Company's personnel files. These files are located in the Human Resources Department and access to the files is limited to members of the HR Department. The Human Resources Director will only allow other staff such as your manager to view or copy information an individual's personnel file if it is essential for them to carry out their duties of employment.

8.3 Accurate and Up to Date Information

The Company will take steps to ensure that the employee information and other personal data it holds is accurate and up-to-date. For example, from time to time you will be asked to inform the Company of any changes which need to be made to update the information held on you, e.g. change of address (although you are also welcome to review and update the information held about you more or less frequently, as you wish).

Please see Section 7.1 of this Policy for more information about your rights of access under the Act to the personal data the Company holds about you.

The Company will also takes steps to ensure that it does not keep any information about employees for longer than is necessary. It may, for example, keep details of employees for a reasonable time after they have left the Company's employment. The Company needs to do this in order to ensure benefits have been properly administered, to give references if requested to do so, to ensure that the Company's tax obligations have been satisfied and to deal with any tribunal or other court proceedings. The Company will retain such records after termination of employment in accordance with its policy on the retention of records or other investigations by authorised bodies.

8.4 Transfer of Personal Data to Others

As a member of the RTL Group of companies, the Company may from time to time need to make employee personal data available to other members of the RTL Group of companies for the purposes set out in this Policy. Likewise, the Company will also need to make employee information available to legal and regulatory authorities (such as HM Revenue and Customs or UK Visas and Immigration), to accountants, auditors, lawyers and other outside professional advisers, and to companies who provide products and services to the Company (such as IT systems suppliers, pension scheme, life assurance or medical benefit providers and intermediaries/brokers, the company which carries out driving licence checks on the 'Company's behalf and other benefit providers) ("Recipients").

Although most Recipients are located in countries within the European Economic Area, others may be located, or have relevant operations elsewhere. Therefore it may be necessary for the Company to transfer your personal data to countries outside the European Economic Area, in particular to the United States. Some of these countries may not have laws regulating the use and transfer of personal data. In this case, the Company will take steps to ensure that the Recipients whether internal or external, observe the principles set out in this Policy.

9. Your Rights and Responsibilities under the Data Protection Act

9.1 Data Protection Rights

The Act gives employees (and anyone else about whom personal data is held) specific rights in relation to some of the information that is held about them. Some of these rights are summarised below, but if you would like any further information, please contact your HR Department.

Under the Act, you are able to:

- obtain confirmation that the Company holds personal data about you, as well as a written description of the information, the purposes for which it is being used, the sources of the information (if available) and the details of any Recipients;
- make a written request to access the personal data which is held about you. *It is important to note that this is not an absolute right to review all the information that is held about you, as there are various exceptions to this right*. One of the most important exceptions is that you may not be able to access the information about you if this would reveal personal information about someone else. In addition, the data may not be readily accessible, the information you seek may not amount to personal data under the Act or the data may not be held in a relevant filing system.
- ask, in certain circumstances, for the deletion or rectification of personal data which the Company holds about you which is not accurate.

Please contact your HR Department if you want more information about how to exercise these rights. The Company's policy on data subject access to company information are explained in detail in the Company's Subject Access Request Policy.

9.2 Your Responsibilities

As well as having rights under the Act, all employees must also comply with data protection principles set out in Section 2 of this Policy. Employees must also take steps to ensure that they follow the Company's guidelines on data protection set out in this Policy and in particular, those set out in Section 7.4.

9.3 Your Personal Information

To assist the Company in ensuring that your personal information is kept up to date, you should inform your HR Department of any changes in the following information:

- Address and other contact details;
- Emergency contact name;
- Bank account details;
- Marital or civil partnership status.

9.4 Other People's Personal Information

It may be that as part of your job, you hold personal data about the Company's employees or about other individuals (eg viewers, artists, contributors or business contracts) or are asked to disclose it by others. For example, if you have any managerial responsibility for other employees you are likely to hold personal data about them. You may also be sent a CV containing personal information or you may be disposing of some hard copy documents containing such information. Even if you do not have direct involvement with personal data as part of your job, there may be times when you are asked by others to supply personal data. Therefore, all employees must follow the guidelines set out below.

Please note that the following guidelines apply equally to documents containing personal information which are kept in manual files, as well as information which is kept on a computer database or in any other electronic form.

- All personal information must be kept securely and should remain confidential.
- If you receive a request from someone inside or outside the Company to give them any personal data about an employee (or other individual) you should refer them to the HR Department. The Company needs to verify the identity of the person making such a request and has to balance various considerations when deciding whether and how to respond to such request, including compliance with the Data Protection Act. It is therefore important to refer such requests to the HR Department so that they can ensure the Company's obligations are complied with.

In no circumstances should you give the information to the person requesting such information without first referring the matter to the HR Department and getting prior written approval. You may be requested to verify the identity of the person making the request or be asked to seek further clarification of the reasons why the information is needed, before the request can be considered.

- You should be aware that it is a **criminal offence** under the Act if you deliberately or recklessly disclose personal data to someone outside the Company without the Company's consent.
- Accessing, disclosing or otherwise using employee records or other employee personal data without authority will be treated as a serious disciplinary offence and may result in disciplinary action being taken in accordance with the Company's Disciplinary Rules and Procedure.
- If you do need to send personal data to a third party, and have been authorised to do so, avoid sending personal data which is confidential by e-mail/other electronic means unless you are sure that the link is secure and confidential. For example, you may need to encrypt e-mail and alert the recipient to indicate to them to also keep the information secure and confidential.
- You should not keep personal data about people which you no longer need or which is out of date or inaccurate. You should therefore review any personal data that you hold from time to time, bearing these principles in mind.

You should find it easier to comply with these requirements if you follow the Employee Data Protection Guidelines about keeping the information confidential which are attached to this policy.

If you are unsure about the application of these guidelines to the information you hold as part of your job, you should contact your HR Department for further guidance.

This Policy is provided by way of guidance only and does not form part of your contract of employment with the Company. The Company may issue further guidance or amendments to this Policy from time to time and/or in line with legal developments.

10. APPENDIX 1: EMPLOYEE DATA PROTECTION DO'S AND DON'TS

10.1 STORING DATA

DO's:

- Try and scan shared copy documents containing personal data to create an electronic record where possible, so that the information is held securely on the company's network.
- Keep paper files containing personal information in filing cabinets or pedestals and check that such cabinets/pedestals are locked before you leave the office.
- Follow the rules on Passwords and computer security set out in the "Data Security & Protection Guidelines" document produced by IT.
- Password protect any documents containing particularly sensitive personal information about anyone.
- Take extra care if you take your work home or away from the office where there is a greater risk of loss, theft or damage to personal information. Password protect Word/Excel documents where possible and keep your laptop in a secure location at all times.
- Inform IT Support Helpdesk on Ex 6996 as soon as possible if either a mobile phone, laptop or any other equipment on which you do company work, even if this is personal IT equipment, has been lost or stolen.
- Set a PIN on any mobile phone you are doing work on, so that if it is lost or stolen, the company's data will be protected. Please contact IT Support Helpdesk on Ex 6996 in IT if you are unsure how to do this.
- Report all computer security incidents including virus infections to IT Support Helpdesk on Ex 6996.
- Follow the general guidance on handling personal information issued by the Privacy Office.

DON'T's:

- Leave your work laptop or work mobile phone unattended at any time outside the office. Remember that you are responsible for ensuring that all personal data held by you is kept secure.

- Use an external device, including discs and other data storage devices such as USB sticks, to store personal data without prior notification to the IT department. Always ensure that all such portable devices are password protected.
- Leave CVs or any other papers containing personal data lying around your desk. Keep such information in locked filing cabinets or pass it on to your Human Resources Department where it relates to an existing employee/destroy in accordance with the Retention Policy.
- Take hard copy documents containing personal data home with you unless you are sure they can be stored securely at home.

10.2 SHARING DATA

DO's:

- Send all information on employees such as CVs, appraisals, compensation details or health records to the HR Department where it will be held securely.
- Check all the recipients of your emails before you press send. You don't want to send someone's personal information to the wrong recipient by accident. If you do send someone's personal information to the wrong recipient, let your line manager know. All personal data breaches must be reported.
- Only print out confidential information when necessary.
- Seek assistance from your legal department before entering into any contractual relationship with service providers.
- Keep your IT systems password safe. Do not disclose it to anyone. If you are going on holiday or are going to be away from the office, ensure you change your password upon your return to the office.
- Be wary of people who may try and trick you into disclosing over the phone or by e-mail personal details about a staff member.
- If someone requests details about personal information that Fremantle holds about them, refer the request to the relevant legal team or Privacy Office if you are unsure who the relevant legal team are. The identity of the requester must be verified and the personal information we send out needs to be checked by the relevant legal team or Privacy Office if you are unsure who the relevant legal team are. Refer to our Subject Access Request Policy for further details.

DON'T's:

- If someone asks you to disclose personal information over the telephone (whether about you or a third party), don't disclose it! If you are unsure about the identity of the

caller, ask him/her to put their request in writing or in an e-mail. If you receive a request for personal information about an employee, please pass it on to your Human Resources Department.

10.3 DELETING OR DESTROYING DATA

DO's:

- Delete or destroy any records that have passed their retention period – refer to our Record Retention Period Index.
- When you are disposing of paper files or documents containing personal information, you MUST always either shred them or discard them as confidential waste in the secure disposal bins located on your floor. These are the tall red/blue bins on wheels that have their lids sealed with security cable ties.
- Delete documents and emails containing personal information off any device where they are no longer needed. For example, delete any contact lists (e.g. email contact lists) you no longer need.
- Set regular times for all files to be reviewed to see if anything can be archived, destroyed or deleted.
- If your employment with Fremantle ends (as a contractor or permanent employee), hand in all company-issued property (including laptops and work mobile phones) and delete any Fremantle data off your personal devices (including work emails).

DON'T's:

- Hold onto documents or emails containing personal information when you no longer need that personal information. Delete or destroy unneeded personal information securely.
- Delete or destroy any legal documents (including releases) without consulting with your line manager. All legal documents should be kept for a minimum period of 7 years.

11. Appendix 2: Data Protection Do's and Don't's for Production Staff

11.1 The most up-to-date list of Do's and Don'ts for PRODUCTION STAFF are available in Knowledge Hub at:

https://fremantlemedia.sharepoint.com/sites/knowledgehub