GRAVITY MEDIA PRIVACY STANDARD

GRAVITY MEDIA (AUSTRALIA) PTY LTD, TRADING AS GRAVITY MEDIA

PRIVACY STANDARD

CONTENTS

1. INTRODUCTION

This Privacy Standard sets out how Gravity Media Group Limited, trading as Gravity Media ("**we**", "**our**", "**us**", "**Gravity Media**") handle the Personal Information of our employees, workers and other third parties such as contractors. This policy applies across all companies within the Gravity Media Group.

This Privacy Standard applies to all Personal Information we Process, regardless of the media on which that data is stored or whether it relates to past or present employees, workers, contractors, and shareholders.

This Privacy Standard applies to all Gravity Media Personnel ("**you**", "**your**"). You must read, understand, and comply with this Privacy Standard when Processing Personal Information on our behalf and attend training on its requirements. This Privacy Standard sets out what we expect from you in order for Gravity Media to comply with applicable law. Your compliance with this Privacy Standard is mandatory. Related Policies and Privacy Guidelines are available to help you interpret and act in accordance with this Privacy Standard. You must also comply with all such Related Policies and Guidelines, which consist of the following: Retention Guidelines (schedule 3) and the Information Security Policy. Any breach of this Privacy Standard is a disciplinary matter.

This Privacy Standard (together with Related Policies and Privacy Guidelines listed above) is an internal document and cannot be shared with third parties, clients or regulators without prior authorisation from the Data Protection Officer.

The capitalised terms throughout this policy are as defined in the following clause 2.1.

2. INTERPRETATION

DEFINITIONS:

Company Personnel: all employees, workers, contractors, agency workers, consultants, directors, freelancers, members and others.

Consent: agreement which must be freely given, specific, informed and be an unambiguous indication of the Data Subject's wishes by which they, by a statement or by a clear positive action, signifies agreement to the Processing of Personal Information relating to them.

Data Controller: the person or organisation that determines when, why and how to process Personal Information. We are the Data Controller of all Personal Information relating to our Gravity Media Personnel and Personal Information used in our business for our own commercial purposes.

Data Protection Officer (DPO): the person responsible for overseeing data protection strategy and implementation to ensure compliance with data protection regulations such as Australia's Privacy Act 1988. Gravity Media's DPO can be contacted at *grp-uk-data_protection@gravitymedia.com*.

Data Subject: a living, identified or identifiable individual about whom we hold Personal Information. Data Subjects may be nationals or residents of any country and may have legal rights regarding their Personal Information.

Data Privacy Impact Assessment (DPIA): tools and assessments used to identify and reduce risks of a data processing activity. DPIA can be carried out as part of Privacy by Design and should be conducted for all major system or business change programs involving the Processing of Personal Information.

Explicit Consent: consent which requires a very clear and specific statement (that is, not just action).

Australia's Privacy Act 1988/Australia Privacy Principles ("APPs"): Australia's Privacy Act 1988 provides a set of principles to be applied when working with personal information. These are known as the Australian Privacy Principles ("APPs"). Among other things, they provide rules about transparency, direct marketing, and security of personal information.

Personal Information: any information identifying a Data Subject or information relating to a Data Subject that we can identify (directly or indirectly) from that data alone or in combination with other identifiers we possess or can reasonably access. Personal Information includes Sensitive Information and Pseudonymised Information but excludes anonymous data or data that has had the identity of an individual permanently removed. Personal Information can be factual (for example, a name, email address, location or date of birth) or an opinion about that person's actions or behaviour.

Personal Information Breach: any act or omission that compromises the security, confidentiality, integrity or availability of Personal Information or the physical, technical, administrative or organisational safeguards that we or our third-party service providers put in place to protect it. The loss, or unauthorised access, disclosure or acquisition, of Personal Information is a Personal Information Breach.

Privacy by Design: implementing appropriate technical and organisational measures in an effective manner to ensure compliance with Australia's Privacy Act 1988.

Privacy Guidelines: The Company privacy/APPs related guidelines provided to assist in interpreting and implementing this Privacy Standard and Related Policies, available in this document.

Privacy Notices: separate notices setting out information that may be provided to Data Subjects when Gravity Media collects information about them. A template Privacy Notice is attached at schedule 1.

Processing: any activity that involves the use of Personal Information. It includes obtaining, recording or holding the data, or carrying out any operation or set of operations on the data including organising, amending, retrieving, using, disclosing, erasing or destroying it. Processing also includes transmitting or transferring Personal Information to third parties.

Pseudonymisation or Pseudonymised: replacing information that directly or indirectly identifies an individual with one or more artificial identifiers or pseudonyms so that the person, to whom the data relates, cannot be identified without the use of additional information which is meant to be kept separately and secure.

Sensitive Information: information revealing racial or ethnic origin, political opinions, religious or similar beliefs, trade union membership, physical or mental health conditions, sexual life, sexual orientation, biometric or genetic data, and Personal Information relating to criminal offences and convictions.

Scope

We recognise that the correct and lawful treatment of Personal Information will maintain confidence in the organisation and will provide for successful business operations. Protecting the confidentiality and integrity of Personal Information is a critical responsibility that we take seriously at all times.

All directors, managers, and heads of business units are responsible for ensuring all Gravity Media Personnel comply with this Privacy Standard and need to implement appropriate practices, processes, controls and training to ensure such compliance.

The Data Protection Officer (DPO) is the person responsible for overseeing this Privacy Standard and, as applicable, developing Related Policies and Privacy Guidelines. Gravity Media's DPO can be contacted at grp-uk-data_protection@gravitymedia.com.

Please contact the DPO with any questions about the operation of this Privacy Standard or the APPs or if you have any concerns that this Privacy Standard is not being or has not been followed.

How Gravity Media collects information

Gravity Media may collect personal information about an individual in the following circumstances:

- when they commence employment with Gravity Media
- when they enter into a contract with Gravity Media
- when they engage with Gravity Media for the provision of services.
- when they interact or conduct business with Gravity Media
- when they use the Gravity Media website; or
- When they register to receive Gravity Media newsletters and other communications.

As well as collecting information directly from an individual, there may be occasions when Gravity Media collects information from a third party which will supplement the information held by Gravity Media. These third parties may include related bodies corporate (as defined in the Corporations Act 2001 (Cth)) of Gravity Media ("Group Companies") which includes entities incorporated in the United Kingdom.

How Gravity Media stores information

Personal information is stored and held in a combination of hard copy and electronic employee files maintained by Gravity Media. Personal information is only accessible by officers and employees of Gravity Media and its Group Companies, unless it is disclosed to another party in accordance with this Policy.

Gravity Media takes all reasonable steps to protect personal information from misuse, interference and loss, as well as unauthorised access, modification or disclosure by using industry standard software protection programs.

How is personal information used?

Personal information is used by Gravity Media to service and assist employees, contractors, and other individuals.

Gravity Media does not generally engage in direct marketing with individuals, however if personal information is to be used for direct marketing purposes, then section 5 (direct marketing) of this Policy will apply.

Disclosure of information

Personal information may be disclosed to employees and agents of Gravity Media and its Group Companies, to enable them to administer accounts, products and services provided by Gravity Media and/or its Group Companies.

Personal information may be sent by Gravity Media to the United Kingdom, United States of America, France, Germany, and Qatar for storage and use by Group Companies. Section 3.13(m) (cross-border disclosure of personal information) of this Policy will apply if any personal information is to be disclosed to an overseas entity.

3. PERSONAL INFORMATION PRIVACY OBLIGATIONS

We adhere to the privacy obligations relating to the Processing of Personal Information set out in the APPs. Set out below are the procedures that Gravity Media must comply with them collecting, storing, and using Personal Information.

a) Collection of solicited personal information.
b) Anonymity and pseudonymity.
c) Sources of Personal Information.
d) Individual entitled to certain details.
e) Collection of Sensitive Information.
f) Use and disclosure of Personal Information.
g) Quality of Personal Information.
h) Security of information.
i) Information that is no longer required.
j) Request for access to Personal Information.
k) Request for correction of Personal Information.
l) Adoption, use of disclosure of government related identifiers.
m) Cross-border disclosure of Personal Information.

We are responsible for and must be able to demonstrate compliance with the data protection obligations listed above.

(a) Collection of solicited Personal Information.

Personal Information must be Processed lawfully, fairly and in a transparent manner in relation to the Data Subject.

Personal Information is only to be collected from clients, customers, suppliers, employees, or other parties for one or more of Gravity Media's functions or activities. Please consider before collecting information whether any request for information you make will satisfy this test.

Personal Information must only be collected by lawful and fair means, and not in an intrusive manner.

You must identify and document the legal ground being relied on for each Processing activity.

(b) Anonymity and Pseudonymity.

If lawful and possible to do so, allow people the option of interacting with Gravity Media anonymously, or by using a pseudonym. However, this will not usually be appropriate, particularly in the case of clients and employee payroll purposes.

(c) Sources of Personal Information

Collect Personal Information directly from the individual, if it is reasonable and practicable to do so, rather than collecting information indirectly (e.g. from third parties). When collecting Personal Information or receiving Personal Information (including receipt of information from a third party), the source of Personal Information must be recorded and retained with the Personal Information.

(d) Individuals entitled to certain details.

The APPs requires us to provide detailed, specific information to Data Subjects depending on whether the information was collected directly from Data Subjects or from elsewhere. Such information must be provided through appropriate

Privacy Notices which must be concise, transparent, intelligible, easily accessible, and in clear and plain language so that a Data Subject can easily understand them. A template Privacy Notice is at Schedule 1.

Whenever we collect Personal Information directly from Data Subjects, including for human resources or employment purposes, we must provide the Data Subject with all the information required by the APPs including the identity of the Data Controller and DPO, how and why we will use, Process, disclose, protect and retain that Personal Information through a Privacy Notice which must be presented when the Data Subject first provides the Personal Information.

That individual is entitled to be made aware of certain details including:

- The identity of Gravity Media and its contact details.
- The purpose for collecting the information.
- The fact that they are able to gain access to the information.
- The fact that they are able to make a complaint.
- The organisations to which Gravity Media usually discloses information of that kind.
- Whether disclosure is likely to overseas recipients and, if so, the relevant countries where information will be disclosed.
- Any law requiring that information to be collected; and
- The main consequences (if any) for the individual if he/she does not provide all or part of the information.

It is important that all Gravity Media staff provide the above details to individuals in a complete and accurate manner. If you are unsure about any of the above, you should consult the DPO. Providing the individual with incorrect details, for example, misstating the purposes for collecting the information, may expose Gravity Media to liability in certain circumstances.

When Personal Information is collected indirectly (for example, from a third party or publicly available source), you must provide the Data Subject with all the information required by the APPs as soon as possible after collecting/receiving the data.

(e) Collection of Sensitive Information.

Unless a specific exemption applied, Gravity Media must not collect Sensitive Information unless the relevant individual has consented to the collection, and the information is reasonably necessary for one or more of Gravity Media's functions or activities. Sensitive Information is personal or health information regarding an individual's racial or ethnic origin, political opinions, membership of a political association, religious beliefs or affiliations, philosophical beliefs, membership of a professional or a trade association, membership of a trade union, sexual preferences or practices or criminal record.

(f) Use and disclosure of Personal Information

Personal Information must be collected only for specified, explicit and legitimate purposes. It must not be further Processed in any manner incompatible with those purposes.

You cannot use Personal Information for new, different, or incompatible purposes from that disclosed when it was first obtained unless you have informed the Data Subject of the new purposes and they have Consented where necessary.

Gravity Media must only use or disclose Personal Information for the primary purpose for which Gravity Media has collected it and not for any secondary purpose, unless:

- Gravity Media has obtained the individuals' consent. This can be express or implied. Implied consent is where it can reasonably be inferred by an individual's conduct.
- There is a serious threat to an individual's life, health, or safety.
- Gravity Media is required or authorised to disclose Personal Information by law or to enforcement bodies, for example, in relation to criminal investigations.
- It will assist to locate a person who has been reported as missing; or
- The direct marketing exception applies (please see separate section below).

Gravity Media can help to avoid complaints from individuals and misunderstandings of the primary purpose or what would reasonably be expected to be done with information by ensuring that individuals are accurately information about the intended primary purpose and proposed uses and disclosures at all times.

(g) Quality of Personal Information

Personal Information must be accurate and, where necessary, kept up to date. It must be corrected or deleted without delay when inaccurate.

You will ensure that the Personal Information we use, and hold is accurate, complete, kept up to date and relevant to the purpose for which we collected it. You must check the accuracy of any Personal Information at the point of collection and at regular intervals afterwards. You must take all reasonable steps to destroy or amend inaccurate or out-of-date Personal Information.

Personal Information must not be kept in an identifiable form for longer than is necessary for the purposes for which the data is processed.

You must not keep Personal Information in a form which permits the identification of the Data Subject for longer than needed for the legitimate business purpose or purposes for which we originally collected it including for the purpose of satisfying any legal, accounting or reporting requirements.

Gravity Media will maintain the Data Retention Guidelines at Schedule 2 to ensure Personal Information is deleted after a reasonable time for the purposes for which it was being held, unless a law requires such data to be kept for a minimum time.

You will take all reasonable steps to destroy or erase from our systems all Personal Information that we no longer require in accordance with all Gravity Media's applicable records retention schedules and policies. This includes requiring third parties to delete such data where applicable.

You will ensure Data Subjects are informed of the period for which data is stored and how that period is determined in any applicable Privacy Notice.

(h) Security of Information

Personal Information must be secured by appropriate technical and organisational measures against unauthorised or unlawful Processing, and against accidental loss, destruction, or damage.

We will develop, implement, and maintain safeguards appropriate to our size, scope and business, our available resources, the amount of Personal Information that we own or maintain on behalf of others and identified risks (including use of encryption and Pseudonymisation where applicable). We will regularly evaluate and test the effectiveness of those safeguards to ensure security of our Processing of Personal Information. You are responsible for protecting the Personal Information we hold. You must implement reasonable and appropriate security measures

against unlawful or unauthorised Processing of Personal Information and against the accidental loss of, or damage to, Personal Information. You must exercise particular care in protecting Sensitive Information from loss and unauthorised access, use or disclosure.

You must follow all procedures and technologies we put in place to maintain the security of all Personal Information from the point of collection to the point of destruction. You may only transfer Personal Information to third-party service providers who agree to comply with the required policies and procedures and who agree to put adequate measures in place, as requested.

You must maintain data security by protecting the confidentiality, integrity and availability of the Personal Information, defined as follows:

a) Confidentiality means that only people who have a need to know and are authorised to use the Personal Information can access it.
b) Integrity means that Personal Information is accurate and suitable for the purpose for which it is processed.
c) Availability means that authorised users are able to access the Personal Information when they need it for authorised purposes.

You must comply with all applicable aspects of our Information Security Policy.

(i) Information that is no longer required

If Gravity Media no longer needs the Personal Information for any purpose for which it may use or disclose the information (e.g. if the primary purpose for collection is no longer relevant) and the information is not otherwise required to be kept under an Australian law or court order, you must take reasonable steps to destroy or permanently de-identify the information.

(j) Request for access to Personal Information

Upon request, Gravity Media must give an individual access to the information that Gravity Media holds about him/her, unless specific limitations apply (for example, if the request is frivolous or vexatious, or providing access would be unlawful). Gravity Media reserves the right to charge reasonable costs incurred in providing this access, and individuals making requests for access should be informed of this. Gravity Media may deny a request for access in circumstances where:

- the request is frivolous or vexatious.
- providing access would pose a threat to the life, health or safety of any person or to public health or public safety.
- providing access would have an unreasonable impact upon the privacy of other persons.
- providing access would prejudice negotiations involving that person or likely prejudice an investigation of possible unlawful activity, or misconduct of a serious nature or other activities by enforcement bodies.
- providing access would reveal evaluative information generated within Gravity Media in connection with a commercially sensitive decision-making process and an explanation for the decision can be provided rather than the information itself.
- providing access would reveal information relating to existing or anticipated legal proceedings between Gravity Media and the individual that would not be accessible by the process of discovery in those proceedings.
- providing access would be unlawful; or
- Denying access is required or authorised by or under an Australian law or a court / tribunal order.

Gravity Media must respond to a request for access to personal information within a reasonable period after the request is made and give access to the information in the manner requested by the individual if it is reasonable and practicable to do so.

If Gravity Media denies access to the personal information, it must give the individual a written notice that sets out:

- the reasons for the refusal except to the extent that, having regard to the grounds for the refusal, it would be unreasonable to do so; and
- The mechanisms available to complain about the refusal.

(k) Request for correction of Personal Information

A person may request Gravity Media to correct the personal information Gravity Media holds about him/her if the person feels it is incorrect. If an individual requests Gravity Media to correct the information, Gravity Media must take such steps (if any) as are reasonable in the circumstances to correct that information to ensure that, having regarding to the purpose for which it is held, the information is accurate, up to date, complete, relevant and not misleading.

Gravity Media must respond to a request for correction of personal information within a reasonable period after the request is made.

If Gravity Media refuses to correct the personal information as requested by an individual, Gravity Media must give the individual a written notice that sets out:

- the reasons for the refusal except to the extent that it would be unreasonable to do so; and
- The mechanisms available to complain about the refusal.

If Gravity Media refuses to correct the personal information, it must keep with the record an indication that the person has requested that the information be corrected.

(l) Adoption, use or disclosure of government related identifiers

Gravity Media must not adopt a government-assigned identifier of the individual (for example, a Tax File Number or Medicare Number) as Gravity Media own identifier of that individual, unless certain circumstances exist which allow you to do so.

(m) Cross-border disclosure of Personal Information

Gravity Media may transfer personal information to a foreign recipient (including when an overseas entity accesses the information in Australia), only if:

- Gravity Media reasonably believes that:
    - the recipient is subject to law, or binding scheme, that has the effect of protecting the information in a way that, overall, is at least substantially similar to the APPs; and
    - there are mechanisms that the individual can access to take action to enforce that protection of the law or binding scheme; or
- The disclosure is required or authorised by or under an Australian law or a court/tribunal order; or
- the transfer is necessary for the performance of a contract with the individual (from which the information was collected); or
- The transfer is for the benefit of the individual (and the other APP requirements are met); or

- If the individual consents to the transfer.

When disclosure is to be made to a known overseas entity, Gravity Media will take reasonable steps to assess the privacy laws of the country where information will be disclosed, to determine whether the overseas recipient is required to comply with privacy laws that are at least as stringent as the APP requirements in relation to information. Gravity Media may enter into a written contract with the overseas recipient to enable Gravity Media to enforce protection of the personal information that it provides to the overseas recipient and ensure that the overseas entity does not breach the APPs.

4. PRIVACY BY DESIGN AND DATA PROTECTION IMPACT ASSESSMENT (DPIA)

It is best practice to implement Privacy by Design measures when Processing Personal Information by implementing appropriate technical and organisational measures (like Pseudonymisation) in an effective manner, to ensure compliance with data privacy obligations.

You must assess what Privacy by Design measures can be implemented on all programs/systems/processes that Process Personal Information by taking into account the following:

a) the state of the art.
b) the cost of implementation.
c) the nature, scope, context and purposes of Processing; and
d) the risks of varying likelihood and severity for rights and freedoms of Data Subjects posed by the Processing.

It is best practice for Data controllers to conduct DPIAs in respect to high risk Processing.

You should conduct a DPIA (and discuss your findings with the DPO) when implementing major system or business change programs involving the Processing of Personal Information including:

e) use of new technologies (programs, systems or processes), or changing technologies (programs, systems or processes).
f) large scale Processing of Sensitive Data; and
g) large scale, systematic monitoring of a publicly accessible area.

A DPIA must include:

h) a description of the Processing, its purposes and the Data Controller's legitimate interests if appropriate.
i) an assessment of the necessity and proportionality of the Processing in relation to its purpose.
j) an assessment of the risk to individuals; and
k) the risk mitigation measures in place and demonstration of compliance.

5. DIRECT MARKETING

Use of personal information for direct marketing

Personal information must not be used by Gravity Media for direct marketing, unless Gravity Media:

- obtains consent of the individual (where information is collected directly from an individual and a relationship exists between the individual and organisation, implied consent will likely be found).
- allows individuals to opt-out from direct marketing communications and this is clearly provided together with Gravity Media's address and telephone number (or some other means to directly contact Gravity Media); and

- Provides the source of the information upon request (free of charge).
- Where information is collected directly from an individual, that information may only be used by Gravity Media for direct marketing if the individual would reasonably expect Gravity Media to do so. Otherwise, information may only be used for direct marketing if in each direct marketing communication, the organisation tells the individual that he or she may request to no longer receive direct marketing.

Sensitive information

Gravity Media must in every case, obtain an individual's explicit consent before using their "sensitive" information for direct marketing.

Recording the source of information

When Gravity Media receives information that it intends to use for direct marking purposes, the source of the information must be recorded, and these records must be maintained. A recipient of unsolicited direct marketing will be able to ask the sender of that direct marketing where they obtained the individual's personal information.

Request to use personal information for direct marketing

Individuals are able to request that Gravity Media not use or disclose their personal information to facilitate direct marketing by other organisations. If Gravity Media receives such a request, Gravity Media must, as soon as possible, comply with the request.

Sharing Personal Information

Generally, we are not allowed to share Personal Information with third parties unless certain safeguards and contractual arrangements have been put in place.

You may only share the Personal Information we hold with another employee, agent or representative of the Gravity Media (which includes our subsidiaries and our ultimate holding company along with its subsidiaries) if the recipient has a job-related need to know the information and the transfer complies with any applicable cross-border transfer restrictions.

You may only share the Personal Information we hold with third parties, such as our service providers if:

a) they have a need to know the information for the purposes of providing the contracted services.
b) sharing the Personal Information complies with the Privacy Notice provided to the Data Subject and, if required, the Data Subject's Consent has been obtained.
c) the third party has agreed to comply with the required data security standards, policies and procedures and put adequate security measures in place.
d) the transfer complies with any applicable cross border transfer restrictions; and
e) a fully executed written contract that contains APPs approved third party clauses has been obtained.

6. DEALING WITH UNSOLICITED INFORMATION

If Gravity Media receives unsolicited Personal Information (being information that it did not ask for), Gravity Media must within a reasonable period of time, determine whether, if Gravity Media had sought the information, it could have collected the information lawfully.

If Gravity Media determines that the Personal Information could not have been collected lawfully, it must have soon as practicable but only if it is lawful and reasonable to do so, destroy the information or de-identify the information.

If the Personal Information could have been collected lawfully, this Policy applies as if the information has been collected in that lawful manner.

7. SECURITY BREACHES

We have put in place procedures to deal with any suspected Personal Information Breach and will notify Data Subjects or any applicable regulator where we are legally required to do so.

If you know or suspect that a Personal Information Breach has occurred, do not attempt to investigate the matter yourself. Immediately contact the DPO at *grp-uk-data_protection@gravitymedia.com*, the information technology department and the legal department. You should preserve all evidence relating to the potential Personal Information Breach.

8. WHO CAN I CONTACT FOR FURTHER INFORMATION OR TO MAKE A COMPLAINT?

Individuals are able to contact Gravity Media and request further information about this Policy, request access to their personal information, make a request that personal information be corrected and/or request that personal information be updated. Individuals are also able to make a complaint about any aspect of this Policy, and/or any aspect regarding the collection or use of information by Gravity Media including the following:

- the kind of information collected by Gravity Media.
- the collection process.
- the purpose for which information is collected.
- how information is held; or
- use or disclosure of information by Gravity Media.

Further information can be requested, and complaints can be made using the contact details set out below.

Registered office: Gravity Media (Australia) Pty Ltd

Level 4, 4 Broadcast Way, Artarmon, NSW 2064

Telephone: +61 (0)2 9313 3100

Fax: +61 (0)2 9313 3111

Email: grp-uk-data_protection@gravitymedia.com

Mail: Attention: DPO

Complaints will be investigated by Gravity Media within a reasonable period after the complaint is received. Following an investigation, a response will be provided by Gravity Media to the individual.

If a person is not satisfied with the way in which Gravity Media handles an enquiry or complaint, they can contact the Office of the Australian Information Commissioner on 1300 363 992.

9. CHANGES TO THIS PRIVACY STANDARD

We reserve the right to change this Privacy Standard at any time without notice to you so please check back regularly to obtain the latest copy of this Privacy Standard. This Privacy Standard does not override any applicable national data privacy laws and regulations in countries where a particular company of Gravity Media operates.

10. COMPLIANCE WITH THIS PRIVACY STANDARD

You must comply with all clauses contained in this Privacy Standard and follow the guidelines contained in supporting documents (the Data Retention Guidelines, the Information Security Policy).

11. SCHEDULE 1: PRIVACY NOTICE

[ ] is committed to protecting the privacy and security of your personal information. This privacy notice describes how we collect and use personal information about you during and after your working relationship with us, in accordance with the Australia's Privacy Act 1988/Australia Privacy Principles (APPs). It applies to all employees, workers, and contractors.

[ ] is a "data controller". This means that we are responsible for deciding how we hold and use personal information about you. We are required under data protection legislation to notify you of the information contained in this privacy notice.

This notice applies to current and former employees, workers and contractors. This notice does not form part of any contract of employment or other contract to provide services. We may update this notice at any time but if we do so, we will provide you with an updated copy of this notice as soon as reasonably practical.

It is important that you read and retain this notice, together with any other privacy notice we may provide on specific occasions when we are collecting or processing personal information about you, so that you are aware of how and why we are using such information and what your rights are under the data protection legislation.

Data protection principles

We will comply with data protection law. This says that the personal information we hold about you must be:

1. Used lawfully, fairly and in a transparent way.
2. Collected only for valid purposes that we have clearly explained to you and not in any way incompatible with those.
3. Relevant to the purposes we have told you about and limited only to those purposes.
4. Accurate and kept up to date.
5. Kept only as long as necessary for the purposes we have told you about.
6. Kept securely.

The kind of personal information we hold about you

Personal Information means any information about an individual from which that person can be identified. It does not include anonymous data. There are "special categories" of more Sensitive Information which require a higher level of protection, such as information about a person's health or sexual orientation.

We will collect, store, and use the following categories of **Personal Information** about you:

- Personal contact details such as name, title, addresses, telephone numbers, and personal email addresses.
- Date of birth.
- Gender.
- Marital status and dependants.
- Next of kin and emergency contact information.
- Tax File number.
- Bank account details, payroll records and tax status information.
- Salary, annual leave, pension and benefits information.
- Start date and, if different, the date of your continuous employment.
- Leaving date and your reason for leaving.

- Location of employment or workplace.
- Copy of driving licence.
- Recruitment information (including copies of right to work documentation, references, criminal reports and other information included in a CV or cover letter or as part of the application process).
- Employment records (including job titles, work history, working hours, holidays, training records and professional memberships).
- Compensation history.
- Assessments of your performance, including performance reviews/ratings, performance improvement plans and related correspondence.
- Disciplinary and grievance information which you have been involved, including any warnings issued to you and related correspondence.
- Details of periods of leave taken by you, including holiday, sickness absence/associated medical records, family leave and the reason for the leave,
- CCTV footage and other information obtained through electronic means such as swipe card records.
- Information about your use of our information and communications systems.
- Photographs
- Results of ATO employment status check, details of your interest in and connection with the intermediary through which your services are supplied.

We may also collect, store, and use the following **Sensitive Information**:

- Equal opportunities monitoring information, including information about your race or ethnicity, religious beliefs, and sexual orientation.
- Trade union membership.
- Information about your health, including any medical condition, health, and sickness records, including:
    - where you leave employment and under any share plan operated by a group company the reason for leaving is determined to be ill-health, injury or disability, the records relating to that decision.
    - details of any absences (other than holidays) from work including time on statutory parental leave and sick leave; and
    - where you leave employment and the reason for leaving is related to your health, information about that condition needed for pensions and insurance purposes.
- Information about criminal convictions and offences.

How is your personal information collected?

We collect personal information about employees, workers and contactors through the application and recruitment process from candidates, an employment agency or background check provider, or from you directly. We may sometimes collect additional information from third parties including former employers, credit reference agencies or other background check agencies. We will collect additional personal information in the course of job-related activities through the period you work for us.

Your duty to inform us of changes

It is important that the personal information we hold about you is accurate and current. Please keep us informed if your information changes during your working relationship with us.

How we use Personal Information

We will use your Personal Information in the following circumstances:

1. Where we need to perform the contract, we have entered into with you*
2. Where we need to comply with a legal obligation**
3. Where it is necessary for our/third party legitimate interests and your interests and fundamental rights do not override those interests***

We may also use your Personal Information in the following situations, which are likely to be rare:

4. Where we need to protect your interests (or someone else's interests)
5. Where it is needed in the public interest or for official purposes.

Examples of situations in which we will use your Personal Information

The situations in which we will process your Personal Information are listed below. Some of the grounds will overlap and there may be several grounds justifying our use of your Personal Information. We have indicated by asterisks the above purpose[s] for which we are processing or will process your Personal Information, as well as indicating which categories of data are involved.

- Making a decision about your recruitment or appointment*
- Determining the terms on which you work for us*
- Checking you are legally entitled to work in Australia**
- Paying you and, if you are an employee or deemed employee for tax purposes and deducting tax*
- Providing benefits to you such as pension and healthcare (if applicable) *
- Inviting you to participate in any share plans operated by a group company*
- Enrolling you in a pension arrangement in accordance with our statutory automatic enrolment duties*
- Liaising with the trustees or managers of a pension arrangement operated by a group company, your pension provider and any other provider of employee benefits*
- Administering the contract, we have entered into with you*
- Business management and planning, including accounting and auditing***
- Conducting performance reviews, managing performance and determining performance requirements*
- Making decisions about salary reviews and compensation*
- Assessing qualifications for a particular job or task, including decisions about promotions*
- Gathering evidence for possible grievance or disciplinary hearings*
- Making decisions about your continued employment or engagement or arrangements for the termination of our working relationship*
- Education, training and development requirements*
- Dealing with legal disputes involving you, or other employees, workers and contractors, including accidents at work**
- Ascertaining your fitness to work**
- Managing sickness absence**
- Complying with health and safety obligations**
- To prevent fraud**
- To monitor your use of our information and communication systems to ensure compliance with our IT policies**

- To ensure network and information security, including preventing unauthorised access to our computer and electronic communications systems and preventing malicious software distribution**
- To conduct data analytics studies to review and better understand employee retention and attrition rates**
- Equal opportunities monitoring**
- To apply for passports and visas for travel requirements*
- In order to book travel arrangements for you (including flights, trains, car hire, and taxis)*
- In order to apply for accreditation for projects*

If you fail to provide Personal Information

We may not be able to perform the contract we have entered into with you (paying you or providing a benefit), or we may be prevented from complying with our legal obligations (to ensure the health and safety of our workers).

Change of purpose

We will only use your Personal Information for the purposes for which we collected it, unless we reasonably consider that we need to use it for another reason and that reason is compatible with the original purpose. If we need to use your Personal Information for an unrelated purpose, we will notify you and we will explain the legal basis which allows us to do so.

Please note that we may process your Personal Information without your knowledge or consent, where this is required or permitted by law.

How we use Sensitive Information

Sensitive Information require higher levels of protection. We need to have further justification for collecting, storing and using this type of Personal Information. We may process Sensitive Information in the following circumstances:

1. In limited circumstances, with your explicit written consent.
2. To carry out our legal obligations or exercise rights in connection with employment/engagement.
3. In the public interest, such as equal opportunities monitoring or our occupational pension scheme.

Less commonly, we may process Sensitive Information where it is needed in relation to legal claims or where it is needed to protect your interests (or someone else's interests) and you are not capable of giving your consent, or where you have already made the information public. We may also process such information about members or former members in the course of legitimate business activities with the appropriate safeguards.

Our obligations as an employer

We will use your Sensitive Information in the following ways:

- Information relating to leaves of absence, including sickness absence, family related leaves, or to comply with employment and other laws.
- Information about your physical, mental health, or disability status, to ensure your health and safety in the workplace, assess your fitness to work, provide appropriate workplace adjustments, monitor and manage sickness absence and administer benefits including statutory maternity pay, statutory sick pay, pensions and permanent health insurance.

- If you leave employment and under any share plan operated by a group company and the reason for leaving is determined to be ill-health, injury or disability, we will use information about your physical or mental health, or disability status in reaching a decision about your entitlements under the share plan.
- If you apply for an ill-health pension under a pension arrangement operated by a group company, we will use information about your physical or mental health in reaching a decision about your entitlement.
- Information about your race or national or ethnic origin, religious, philosophical or moral beliefs, or your sexual life or sexual orientation, to ensure meaningful equal opportunity monitoring and reporting.
- We will use trade union membership information to comply with employment law obligations.

Do we need your consent?

We do not need your consent if we use your Sensitive Information to carry out our legal obligations or exercise specific rights in the field of employment law. In limited circumstances, we may approach you for your written consent to allow us to process certain particularly sensitive data. If we do so, we will provide you with full details of the information that we would like and the reason we need it, so that you can carefully consider whether you wish to consent. You should be aware that it is not a condition of your contract with us that you agree to any request for consent from us.

Information about criminal convictions

We may only use information relating to criminal convictions where the law allows us to do so. This will usually be where such processing is necessary to carry out our obligations and provided, we do so in line with our data protection policy. Less commonly, we may use information relating to criminal convictions where it is necessary in relation to legal claims, where it is necessary to protect your interests (or someone else's interests) and you are not capable of giving your consent, or where you have already made the information public. We may also process such information about members or former members in the course of legitimate business activities with the appropriate safeguards.

We envisage that we will hold information about criminal convictions.

Where appropriate, we will collect information about criminal convictions as part of the recruitment process or we may be notified of such information directly by you in the course of you working for us.

Data sharing

We may have to share your data with third parties, including third-party service providers and other entities in the group where required by law, where it is necessary to administer the working relationship with you or where we have another legitimate interest in doing so. We may transfer your personal information to an overseas recipient. If we do, you can expect a similar degree of protection in respect of your Personal Information.

Which third-party service providers process my Personal Information?

Third-party service providers (contractors and designated agents and other entities within the Gravity Media (the "Group")) can include:

- activities carried out by third-party service providers: payroll, pension administration, benefits provision and HR system administration.
- relating to your participation in any share plans operated by a group company with third party administrators, nominees, registrars and trustees for the purposes of administering the share plans; or

- regarding your participation in any pension arrangement operated by a group company with the trustees or scheme managers of the arrangement in connection with the administration of the arrangements.

How secure is my Personal Information with third-party service providers and other entities in our Group?

All our third-party service providers and other entities in the group are required to take appropriate security measures to protect your Personal Information in line with our policies. We do not allow our third-party service providers to use your Personal Information for their own purposes. We only permit them to process your Personal Information for specified purposes and in accordance with our instructions.

When might you share my Personal Information with other entities in the Group?

We will share your Personal Information with other entities in our group as part of our regular reporting activities on company performance, in the context of a business reorganisation or group restructuring exercise, for system maintenance support and hosting of data, relating to your participation in any share plans and pension arrangements operated by a group company with other entities in the Group for the purposes of administering the share plans.

What about other third parties?

We may share your Personal Information with other third parties, for example in the context of the possible sale or restructuring of the business. We may also need to share your Personal Information with a regulator or to otherwise comply with the law. This may include making returns to ATO, disclosures to stock exchange regulators and disclosures to shareholders such as directors' remuneration reporting requirements.

Cross-border disclosure of Personal Information

Gravity Media may transfer personal information to a foreign recipient (including when an overseas entity accesses the information in Australia), only if:

- Gravity Media reasonably believes that:
    - the recipient is subject to law, or binding scheme, that has the effect of protecting the information in a way that, overall, is at least substantially similar to the APPs; and
    - there are mechanisms that the individual can access to take action to enforce that protection of the law or binding scheme; or
- The disclosure is required or authorised by or under an Australian law or a court/tribunal order; or
- the transfer is necessary for the performance of a contract with the individual (from which the information was collected); or
- The transfer is for the benefit of the individual (and the other APP requirements are met); or
- If the individual consents to the transfer.

When disclosure is to be made to a known overseas entity, Gravity Media will take reasonable steps to assess the privacy laws of the country where information will be disclosed, to determine whether the overseas recipient is required to comply with privacy laws that are at least as stringent as the APP requirements in relation to information. Gravity Media may enter into a written contract with the overseas recipient to enable Gravity Media to enforce protection of the personal information that it provides to the overseas recipient and ensure that the overseas entity does not breach the APPs.

Data security

We have put in place measures to protect the security of your information. Details of these measures are available upon request. Third parties will only process your Personal Information on our instructions and where they have agreed to treat the information confidentially and to keep it secure. We have put in place appropriate security measures to prevent your Personal Information from being accidentally lost, used or accessed in an unauthorised way, altered or disclosed. In addition, we limit access to your Personal Information to those employees, agents, contractors and other third parties who have a business need to know. They will only process Personal Information on our instructions, and they are subject to a duty of confidentiality. We have put in place procedures to deal with any suspected data security breach and will notify you and any applicable regulator of a suspected breach where we are legally required to do so.

Data retention

We will only retain your Personal Information for as long as necessary to fulfil the purposes we collected it for, including for the purposes of satisfying any legal, accounting, or reporting requirements. Details of retention periods for different aspects of your Personal Information are available in our retention policy. To determine the appropriate retention period for Personal Information, we consider the amount, nature, and sensitivity of the Personal Information, the potential risk of harm from unauthorised use or disclosure of your Personal Information, the purposes for which we process your Personal Information and whether we can achieve those purposes through other means, and the applicable legal requirements.

In some circumstances we may anonymise your Personal Information so that it can no longer be associated with you, in which case we may use such information without further notice to you. Once you are no longer an employee, worker or contractor of the company we will retain and securely destroy your Personal Information in accordance with our data retention policy and applicable laws and regulations.

Rights of access, correction, erasure, and restriction

Your rights in connection with Personal Information

Under certain circumstances, you have the right to:

- **Request access to your Personal Information**. This enables you to receive a copy of the Personal Information we hold about you and check that we are lawfully processing it.
- **Request correction** of the Personal Information that we hold about you. This enables you to have any incomplete or inaccurate information we hold about you corrected.
- **Request erasure** of your Personal Information. This enables you to ask us to delete or remove Personal Information where there is no good reason for us continuing to process it. You also have the right to ask us to delete or remove your Personal Information where you have exercised your right to object to processing (see below).
- **Object to processing** of your Personal Information where we are relying on a legitimate interest (or those of a third party) and there is something about your particular situation which makes you want to object to processing on this ground. You also have the right to object where we are processing your Personal Information for direct marketing purposes.
- **Request the restriction of processing** of your Personal Information. This enables you to ask us to suspend the processing of Personal Information about you, for example if you want us to establish its accuracy or the reason for processing it.
- **Request the transfer** of your Personal Information to another party.

If you want to review, verify, correct or request erasure of your Personal Information, object to the processing of your Personal Information, or request that we transfer a copy of your Personal Information to another party, please contact the DPO in writing on *grp-uk-data_protection@gravitymedia.com*.

What we may need from you

We may need to request specific information from you to help us confirm your identity and ensure your right to access the information (or to exercise any of your other rights). This is another appropriate security measure to ensure that Personal Information is not disclosed to any person who has no right to receive it.

Right to withdraw consent

In the limited circumstances where you may have provided your consent to the collection, processing and transfer of your Personal Information for a specific purpose, you have the right to withdraw your consent for that specific processing at any time. To withdraw your consent, please contact the DPO on *grp-uk-data_protection@gravitymedia.com*. Once we have received notification that you have withdrawn your consent, we will no longer process your information for the purpose or purposes you originally agreed to, unless we have another legitimate basis for doing so in law.

Data protection officer

We have appointed a data protection officer (DPO) to oversee compliance with this privacy notice. If you have any questions about this privacy notice or how we handle your Personal Information, please contact the DPO on *grp-uk-data_protection@gravitymedia.com*. You have the right to make a complaint at any time to Office of the Australian Information Commissioner (OAIC), the Australian supervisory authority for data protection issues.

Changes to this privacy notice

We reserve the right to update this privacy notice at any time, and we will provide you with a new privacy notice when we make any substantial updates. We may also notify you in other ways from time to time about the processing of your personal information.

Updated on: [ ]

If you have any questions about this privacy notice, please contact the Data Protection Officer at *grp-uk-data_protection@gravitymedia.com*.

[To be accepted electronically]

12. SCHEDULE 2: DATA RETENTION GUIDELINES

1. Introduction

Gravity Media must not retain data for longer than necessary and comply with data protection laws enshrined in the APPs. Data retention has three main principles:

1. Data must only be retained for its intended purpose
2. Data must be kept accurate and up to date
3. Data must be stored securely, whether electronically or on paper.

Records are the multiple data elements which together make up a transaction we have on the system (e.g. supplier details).

2. Purpose

The purpose of this policy is to detail the procedures for the retention and disposal of information to ensure that we carry this out consistently and that we fully document any actions taken. Unless otherwise specified, the data retention guidelines refer to records kept both electronically and on paper.

3. Review

Gravity Media will periodically review retained records to determine if they should be destroyed or retained for a further period.

4. Where do we store our records?

Records are stored electronically in shared folders or in certain business applications (e.g. InspHire or CrewPlanner) which are restricted for use by Gravity Media employees only. Access can only be granted to freelance employees or employees within different departments with managerial approval.

Records in paper form are kept in ring binders or folders within the office, which may be accessed during the day on an employee's desktop. These files must be locked in a cupboard or cabinet when leaving the office overnight and should not be left on a desktop.

5. How long we should keep our records

We should keep any records for as long as they are needed to meet the intended purpose of processing, together with applicable legal and regulatory requirements. We have assessed our records to:

- ascertain whether the documents are valuable as evidence of the activities and purpose of Gravity Media.
- determine their requirement to the business; and,
- establish whether there are any legal or regulatory retention requirements for the records.

A table has been provided with guidelines on how long records should be retained.

6. What you should do when the retention period has expired

If you process data on behalf of any of the companies owned by Gravity Media, and as outlined in the Retention Schedule below, the relevant retention period has expired, you need to review the records you hold and identify whether the data links to a specific client, employee or customer. If it does, you can anonymise or destroy the data.

Data can be anonymised as an alternative to erasing the data completely. This can be done by:

a) Erasing any identifiers (e.g. contact name, address) which link the data to a specific person, or,
b) Separating Personal Information from information which is not unique to a data subject (e.g. having the order number separate from the company name and address).

7. Destruction of data

Records can be destroyed in the following ways:

- Paper records – placed in a shredder
- Electronic records – destroyed on the system and permanently deleted from any backup drives.

8. Data sharing

Multiple copies of the same customer, employee or client data is discouraged, and any duplicate copies should be destroyed. In the event that data has to be shared, only original records should be retained.

If sharing any Personal Information outside Gravity Media, ensure that the data is sent securely and that the third party has adequate procedures in place to ensure records are dealt with according to local and national legislation and regulatory guidance.

9. Monitoring of data retention

Responsibility for monitoring data retention and updating the data retention policy is the responsibility of Gravity Media's Legal Department and, where appropriate, the Data Protection Officer on *grp-uk-data_protection@gravitymedia.com*.

This policy will be reviewed annually.

13. SCHEDULE 3: RETENTION SCHEDULE

Type of Data Record	Department	Retention Period	Manager in Charge of Data Record
Finance			
Financial information (e.g. ledger records, financial accounts, invoices and petty cash records)	Accounts and Finance	6 years	Chief Financial Officer
Expenditure Budgets	Accounts and Finance	6 years (for those submitted to ATO), 2 years (annual estimates used within company)	Chief Financial Officer
Financial Information (on Accpac/Sage)	Accounts and Finance	6 years	Chief Financial Officer
HR			
Employee contracts, Pensions and Retirement information	HR	6 years after the employee has left the organisation or when the pension starts	Chief Human Resources (HR) Officer
Employee salary records	HR	6 years from issue	Chief Human Resources (HR) Officer
Employee training: staff training records	HR	2 years from end of employment	Chief Human Resources (HR) Officer
Employee staff records	HR	6 years after the employee has left the organisation	Chief Human Resources (HR) Officer
Employment recruitment: CVs, JDs, application forms, job offers	HR	Unsuccessful applications – 6 months from job creation date	Chief Human Resources (HR) Officer

Employment: job advertisements	HR	Until superseded	Chief Human Resources (HR) Officer
Legal			
Client contracts (e.g. RFPs and Tenders, service agreements, framework agreements, property owned by Gravity Media)	Legal	6 years after the contract is due to end	Group General Counsel
Litigation with third parties	Legal	Permanent preservation	Group General Counsel
Provision of legal advice	Legal	Permanent preservation	Group General Counsel
Board minutes and agendas	Legal	Whilst active	Group General Counsel
Data Protection: Information rights requests	Legal	6 years from date request satisfied and sent to individual	Group General Counsel
Data Protection: Data incidents and breach management	Legal	6 years from date incident concluded	Group General Counsel
Data Protection: Privacy impact assessments	Legal	6 years from creation date	Group General Counsel
Data Protection: Policies and guidance	Legal	Whilst active	Group General Counsel
Operations			
Accident Book	Office Management	3 years after the last date of entry	Office Manager
RIDDOR reports	Operations	20 years from creation	
Training records	Operations	2 years from end of employment	

Risk Assessments	Operations	Whilst active	
Tax			
Tax records (including income tax records, wages, corporation tax and tax corporate incentives)	Tax/accounts	Up to 3 years after the end of the financial year to which they relate	Tax Director
Projects			
Freelancer contracts	Projects	6 years after contract has ended	Lead Production Manager
Freelancer invoices	Projects	6 years	Lead Production Manager
Staff/Freelancer records: passports, images, new starter forms	Projects	6 years after freelancer has worked for the company	Lead Production Manager
Marketing			
Corporate communications: GMG Live (company news)	Marketing		Head of Marketing
Corporate communications: staff images	Marketing	30 days from leaving employment	Head of Marketing
General correspondence (via GM website)	Marketing	Business need	Head of Marketing
IT			
Staff email addresses	IT	60 days from leaving date	Head of Corporate IT & Cyber Security

Control Sheet

Document reviewer: Carly Thurgood
Document adopted on: 2018
Next review date: July 2023

Review/change history

Date of review/change	Summary of changes	Version no.
July 2022	Addition of control sheet, removal of mention of customers and suppliers, data retention guide amended.	1.0