Staff Privacy Policy and Data Protection Policy

STAFF PRIVACY AND DATA PROTECTION POLICY

PART A - STAFF PRIVACY POLICY

1. GENERAL

1.1 True North Productions Limited (Company Number 04430230 of Marshalls Mill, Marshall Street, Leeds LS11 9YJ) together with any group companies ("we" "us" "our") are committed to protecting and respecting the privacy and security of your personal data. This policy applies to prospective, current and former employees, consultants, directors, secondees, casual workers, agency workers, volunteers and individuals on work experience ("**Staff**").

1.2 The policy describes the categories of personal data that we collect, how we use your personal data, how we secure your personal data, when we may disclose your personal data to third parties, and when we may transfer your personal data outside the United Kingdom. This Privacy Policy also describes your rights regarding the personal data that we hold about you and how you can access, correct, and request erasure of your personal data. We will only process your personal data in accordance with this policy unless otherwise required by applicable law. We take steps to ensure that the personal data that we collect about you is adequate, relevant, not excessive, and processed for limited purposes.

2. COLLECTION AND USE OF PERSONAL DATA

2.1 For the purposes of this privacy policy, personal data means any information about an identifiable individual. Personal data excludes anonymous or de-identified data that is not associated with a particular individual. To carry out our activities and obligations as an employer, we may collect, store, and process the following categories of personal data, which are required for us to administer our relationship (whether as employer, prospective employer or otherwise) with you:

2.1.1 personal contact details such as name, title, addresses, telephone numbers, and personal email addresses;

2.1.2 date of birth;

2.1.3 gender;

2.1.4 marital status and dependants;

2.1.5 next of kin and emergency contact information;

2.1.6 national insurance number;

2.1.7 Bank account details, payroll records, travel logs and expenses and tax status information;

2.1.8 salary, annual leave, pension and benefits information;

2.1.9 start date;

2.1.10 location of employment or workplace;

2.1.11 Information connected with your legal right to drive and/or operate certain machinery e.g. driving licence details;

2.1.12 Recruitment information (including copies of right to work documentation, passport, references and other information included in a CV or cover letter or as part of the application process);

2.1.13 Employment records (including job titles, work history, working hours, training records and professional memberships);

2.1.14 Compensation history;

2.1.15 Performance information;

2.1.16 Disciplinary and grievance information;

2.1.17 Information about your use of our information and communications systems;

2.1.18 Photographs.

2.2 We collect personal information through the application and recruitment process, either directly from candidates or sometimes from an employment agency or online CV database such as Talent Manager. We may sometimes collect additional information from third parties including former employers or other background check agencies. We may collect additional personal information in the course of job-related activities throughout the period of you working for us.

3. USE OF PERSONAL DATA

3.1 We only process your personal data where applicable law permits or requires it, for example, where the processing is necessary for the performance of our employment contract with you, or where the processing is necessary to comply with a legal obligation that applies to us as your employer.

3.2 The table below sets out our reasons for processing your personal data, how those reasons apply to the different types of data we collect (that are listed in paragraph 2.1 above) and the lawful bases we rely for the resulting processing.

Purpose	Type of data	Lawful basis
Making a decision about your recruitment or appointment.	1, 12, 13	Contract
Determining the terms on which you work for us.	1, 8, 9, 12, 13	Contract
Checking you are legally entitled to work in the UK.	1, 2, 6, 11	Legal obligation
Paying you and, if you are an employee, deducting tax and National Insurance contributions.	1, 6, 7, 9	Contract
Providing certain benefits to you.	1, 2, 3, 4, 5, 6, 7, 8, 9	Contract
Liaising with your pension provider.	1, 2, 6, 8, 9	Contract
Administering the contract we have entered into with you.	1, 5, 6, 7, 8 9, 10, 15, 16	Contract
Business management and planning, including accounting and auditing.	1, 2, 3, 6, 7, 8, 9, 10, 15, 16, 17,	Our legitimate interests in operating a television production company
Conducting performance reviews, managing performance and determining	1, 8, 9, 10, 15, 16, 17	Contract

performance requirements.		
Making decisions about salary reviews and compensation.	1, 7, 8, 9, 10, 12, 13, 15, 16, 17	Contract
Assessing qualifications for a particular job or task, including decisions about promotions.	1, 12, 13, 15, 16	Contract
Gathering evidence for possible grievance or disciplinary hearings. Making decisions about your continued employment or engagement.	1, 15, 16, 17, 1, 15, 16, 17	Contract
Making arrangements for the termination of our working relationship.	1, 6, 7, 8, 15, 16	Contract
Education, training and development requirements.	1, 13, 15, 16	Contract
Dealing with legal disputes involving you, or other employees, workers and contractors, including accidents at work.	1, 7, 8, 14, 15, 16, 17, 18,	Our legitimate interests in operating a television production company
Ascertaining your fitness to work and managing sickness absence.	1, 2, 3, 4, 5, 10, 15, 16, 17, 18,	Contract
Complying with	1, 5, 10,	Legal obligation

health and safety obligations.		
To prevent fraud.	1, 6, 7, 11, 12, 13,	Our legitimate interests in operating a television production company
To monitor your use of our information and communication systems to ensure compliance with our IT policies.	1, 17	Our legitimate interests in operating a television production company
To ensure network and information security, including preventing unauthorised access to our computer and electronic communications systems and preventing malicious software distribution.	1, 17	Our legitimate interests in operating a television production company
To conduct data analytics studies to review and better understand employee retention and attrition rates.	1, 2, 3, 4,	Our legitimate interests in operating a television production company
Equal opportunities monitoring.	1, 2, 3, 4,	Consent

3.3 Where we rely on 'legitimate interests' as the lawful basis for processing, such legitimate interests include our legitimate interests in making and exploiting television programmes for worldwide distribution. We only process data on this legal basis where we have considered that, on balance, our legitimate interests or those of a third party are not overridden by your interests, fundamental rights or freedoms.

3.4 We will only process your personal data for the purposes for which we collected it. If we need to process your personal data for an unrelated purpose, we will provide notice to you and, if required by

law, seek your consent. We may process your personal data without your knowledge or consent where required by applicable law or regulation.

3.5 You will not be subject to decisions based on automated data processing without your prior consent.

4. COLLECTION AND USE OF SPECIAL CATEGORY DATA

4.1 Certain categories of personal data may be considered sensitive and may receive special protection including personal data relating to race or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, health, sex life or sexual orientation, genetic data, biometric data (where used for identification purposes) – so called "special category" data - and data about criminal convictions and offences.

4.2 We may collect and process such data where it is necessary for our legitimate interests in operating a television production company and for the purposes of performing or exercising our obligations or rights under employment law, for health purposes, to defend any legal claims that may be brought against us, for reasons of substantial public interest i.e. in relation to equality of opportunity of treatment and for preventing or detecting unlawful acts and in relation to the following categories of sensitive personal data in particular:

4.2.1 trade union membership information in order to:

4.2.1.1 pay trade union premiums;

4.2.1.2 register the status of a trade union representative;

4.2.1.3 facilitate trade union duties and training; and

4.2.1.4 comply with employment law and industrial relations obligations.

4.2.2 biometric data for security purposes, for access to premises and systems and to monitor employee attendance in the work place;

4.2.3 data relating to employee absence for the purpose of absence management procedures;

4.2.4 physical or mental health or condition or disability status including COVID-19 tests results and related symptoms where necessary for reasons of public health and to ensure employee safety in the workplace, provide appropriate

workplace adjustments and to make decisions regarding an employee's fitness to work;

4.2.5 information about employee's racial and ethnic origin; sexual orientation; religion and belief and disability information to ensure meaningful equal opportunity monitoring and reporting; and

4.2.6 criminal offence data contained in criminal record checks which we conduct to ensure we comply with employment law obligations. We will only use your personal data 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. Please contact us if you wish to get an explanation as to how the processing for the new purpose is compatible with the original purpose.

4.3 Please note that we may process your personal data without your knowledge or consent, in compliance with the above rules, where this is required or permitted by law.

5. DISCLOSURE OF YOUR PERSONAL DATA TO THIRD PARTIES

5.1 We will only disclose your personal data to third parties where required by law or to our employees, contractors, designated agents, IT software providers or other third-party service providers who require such information to assist us with administering the employment relationship with you, including third-party service providers who provide services to us or on our behalf. Third-party service providers may include, but not be limited to, payroll processors and benefits administration providers.

5.2 We require all our third-party service providers, by written contract, to implement appropriate security measures to protect your personal data consistent with our policies and any data security obligations applicable to us as your employer. We do not permit our third-party service providers to use your personal data for their own purposes. We only permit them to process your personal data for specified purposes in accordance with our instructions.

5.3 We may also disclose your personal data for the following additional purposes where permitted or required by applicable law:

5.3.1 to other members of our group of companies for the purposes set out in this Privacy Policy and as necessary to perform our employment contract with you;

5.3.2 as part of our regular reporting activities to other members of our group of companies;

5.3.3 to the police, regulatory bodies, legal advisors or similar third parties where we are under a legal duty to disclose or share your personal data in order to comply with any legal obligation. When we disclose your personal data to comply with a legal obligation or legal process, we will take reasonable steps to ensure that we only disclose the minimum personal data necessary for the specific purpose and circumstances;

5.3.4 to any central or local government department and other statutory or public bodies (such as HMRC, DWP) to comply with applicable law;

5.3.5 to a prospective employer of yours who requests a reference;

5.3.6 to protect our the rights and property;

5.3.7 during emergency situations or where necessary to protect the safety of persons;

5.3.8 where the personal data is publicly available;

5.3.9 if a business transfer or change in ownership occurs; and

5.3.10 for additional purposes with your consent where such consent is required by law.

6. INTERNATIONAL TRANSFERS

Where permitted by applicable law, we may transfer the personal data we collect about you to jurisdictions outside the UK that may not be deemed to provide the same level of data protection as the UK, as necessary to perform our employment contract with you and for the purposes set out in this Privacy Policy. If we do transfer your data outside of the UK, we do so on the basis of an adequacy decision or, where this is not available, legally-approved standard data protection clauses recognised or issued further to Article 46(2) of the UK GDPR to ensure your personal data is given the same level of protection. You can find out more about these safeguards by contacting us using the contact details below.

7. DATA SECURITY

All information you provide to us is stored on our secure servers. We have implemented appropriate physical, technical, and organisational security measures designed to secure your personal data against accidental loss and unauthorised access, use, alteration or disclosure. In addition, we limit access to personal data to those employees, agents, contractors and other third parties that have a legitimate business need for such access.

8. RETENTION OF YOUR PERSONAL DATA

Except as otherwise permitted or required by applicable law or regulation, we will only retain your personal data 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 and we will review this from time to time in accordance with the Data Retention Policy. Where you are engaged to work on a production, we will retain your relevant personal information for as long as we need to in order to exploit the production in accordance with our legitimate interests and, where applicable, our legal obligations. In other cases we will normally hold your data for 6 years following the end of your employment or engagement with us. For further details, please check the Data Retention Policy. Under some circumstances we may anonymise your personal data so that it can no longer be associated with you. We reserve the right to use such anonymous and de-identified data for any legitimate business purpose without further notice to you or your consent.

9. RIGHTS OF ACCESS, ERASURE AND OBJECTION

9.1 It is important that the personal data we hold about you is accurate and current. Please keep us informed if your personal data changes during your employment, for example, if you move house or your bank details change. By law you have the right to be informed about the data we hold about you. You also have the right to:

9.1.1 ask us to provide you with a copy of your personal data;

9.1.2 ask us to delete your personal data (in certain situations);

9.1.3 ask us to restrict processing of your personal data in certain circumstances;

9.1.4 ask to receive the personal data you provided to us, in a structured, commonly used and machine-readable format and/or transmit that data to a third party (in certain situations);

9.1.5 to object:

9.1.5.1 at any time to your personal data being processed for direct marketing (including profiling); and

9.1.5.2 in certain other situations to our continued processing of your personal data.

9.1.6 not to be subject to a decision based solely on automated processing that produces legal effect concerning you or similarly significantly affects you;

9.1.7 to withdraw consent at any time if you have provided us with consent to use your personal data.

9.2 If you want to exercise any of these rights please contact Norma Wisnevitz via email – nwisnevitz@truenorth.tv. .

9.3 We may request specific information from you to help us confirm your identity and your right to access, and to provide you with the personal data that we hold about you or make your requested changes. Applicable law may allow or require us to refuse to provide you with access to some or all of the personal data that we hold about you, or we may have destroyed, erased, or made your personal data anonymous in accordance with our record retention obligations and practices. If we cannot provide you with access to your personal data, we will inform you of the reasons why, subject to any legal or regulatory restrictions.

10. CHANGES TO OUR PRIVACY POLICY

10.1 Any changes we may make to our privacy policy in the future will be updated in this Policy. We will notify you if there are any changes to this policy that materially affect how we collect, store or process your personal data. If we would like to use your personal data for different purposes than those we have notified to you at the time of collection, we will provide you with notice and, where required by law, seek your consent, before using your personal data for a new or unrelated purpose. We may process your personal data without your knowledge or consent where required by applicable law or regulation.

11. CONTACT US

11.1 We have appointed Norma Wisnevitz as our Data Protection Manager to oversee compliance with this privacy policy.

11.2 Norma Wisnevitz has the following responsibilities:

11.2.1 Briefing the directors and employees at True North on data protection responsibilities;

11.2.2 Reviewing this Policy and related policies;

11.2.3 Advising other staff on data protection issues;

11.2.4 Ensuring that any relevant training takes place;

11.2.5 Handling subject access requests – if such a request is received please forward to Norma Wisnevitz immediately;

11.2.6 Notification; and

11.2.7 Approving unusual or controversial disclosures of personal data.

11.3 If you have any questions, comments or requests regarding this policy or how we use your personal data please contact Norma Wisnevitz at nwisnevitz@truenorth.tv.This is in addition to your right to contact the Information Commissioners Office if you are unsatisfied with our response to any issues you raise at https://ico.org.uk/global/contact-us/.

PART B – DATA PROTECTION POLICY

1. INTRODUCTION

1.1 This Data Protection Policy sets out how True North Productions Limited ("we", "our", "us", "the Organisation") handle the Personal Data of our customers, suppliers, employees, workers and other third parties.

What is Personal Data?

Personal Data means any information identifying an individual (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. Identifiers can include an identification name, location data or online identification or one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of the individual.

Personal Data includes Special Category Data but excludes anonymous data or data that has had the identity of an individual permanently removed. Personal data can be factual (for example, a name, email address, location or date of birth) or an opinion about that person's actions or behaviour.

1.2 This Data Protection Policy applies to all Personal Data we Process regardless of the media on which that data is stored or whether it relates to past or present employees, workers, customers, clients or supplier contacts, shareholders, website users or any other Data Subject.

What does it mean to 'process' Personal Data?

Process, Processing, or Processed means any activity that involves the use of Personal Data. 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 Data to third parties.

1.3 This Data Protection Policy applies to all employees, workers, contractors, agency workers, consultants, directors, members and others ("Personnel"). You must read, understand and comply with this Data Protection Policy when Processing Personal Data on our behalf and attend training on its requirements. This Data Protection Policy sets out what we expect from you in order for us to comply with applicable law. Your compliance with this Data Protection Policy is mandatory. If you are an employee, any breach of this Data Protection Policy may result in disciplinary action. If you are a non-employee, any breaches of this Data Protection Policy may result in us terminating your contract with immediate effect.

1.4 This policy does not form part of an employee's contract of employment and may be amended from time to time. This Data Protection Policy (together with Related Policies) is an internal document and cannot be shared with third parties, clients or regulators without prior authorisation from the Data Protection Manager/Data Protection Lead.

1.5 This policy has the definitions set out at paragraph 3.1 which apply throughout. Please read these definitions carefully to ensure you understand how they operate in this policy.

2. SCOPE

2.1 We recognise that the correct and lawful treatment of Personal Data will maintain confidence in the Organisation and will provide for successful business operations. Protecting the confidentiality and integrity of Personal Data is a critical responsibility that we take seriously at all times. The Organisation is exposed to potential fines of up to £17.5 million or 4% of total worldwide annual turnover, whichever is higher and depending on the breach, for failure to comply with the provisions of Data Protection Legislation. Personal Data breaches also carry the risk of significant civil and criminal sanctions for individuals and in some circumstances, can amount to a criminal offence.

2.2 This policy sets out how we comply with our data protection obligations and seek to protect Personal Data. Its purpose is also to ensure that our Personnel understand and comply with the rules governing the collection, use and deletion of Personal Data to which they may have access in the course of their work

2.3 All business areas are responsible for ensuring all Personnel comply with this Data Protection Policy and need to implement appropriate practices, processes, controls and training to ensure such compliance.

2.4 The Data Protection Manager is responsible for overseeing this Data Protection Policy and, as applicable, developing Related Policies. That post is held by Norma Wisnevitz. You can contact Norma by email at: nwisnevitz@truenorth.tv

2.5 Please contact the Data Protection Manager with any questions about the operation of this Data Protection Policy or Data Protection Legislation or if you have any concerns that this Data Protection Policy is not being or has not been followed. In particular, you must always contact the Data Protection Manager in the following circumstances:

2.5.1 if you are unsure of the lawful basis which you are relying on to process Personal Data (including the legitimate interests used by the Organisation) (see Section 5.1 below);

2.5.2 if you need to rely on Consent and/or need to capture Explicit Consent (see Section 5.2 below);

2.5.3 if you need to draft Privacy Notices (see Section 5.3 below);

2.5.4 if you need any assistance dealing with any rights invoked by a Data Subject (see Section 6);

2.5.5 if you are unsure about the retention period for the Personal Data being Processed (see Section 10 below);

2.5.6 if you are unsure about what security or other measures you need to implement to protect Personal Data (see Section 11.1 below);

2.5.7 if you need help with any contracts or other areas in relation to sharing Personal Data with third parties (including our vendors) (see Section 11.2 below).

2.5.8 if there has been a Personal Data Breach (Section 11.3 below);

2.5.9 if you are unsure on what basis to transfer Personal Data outside the UK (see Section 11.4 below);

2.5.10 whenever you are engaging in a significant new, or change in, Processing activity which is likely to require a DPIA (see Section 12.4 below) or plan to use Personal Data for purposes others than what it was collected for;

2.5.11 If you plan to undertake any activities involving Automated Processing including profiling or Automated Decision-Making (see Section 12.5 below); or

2.5.12 If you need help complying with applicable law when carrying out direct marketing activities (see Section 13 below).

3. INTERPRETATION

3.1 DEFINITIONS:

Automated Decision-Making (ADM): when a decision is made which is based solely on Automated Processing (including profiling) which produces legal effects or significantly affects an individual. The UK GDPR prohibits Automated Decision-Making (unless certain conditions are met) but not Automated Processing.

Automated Processing: any form of automated processing of Personal Data consisting of the use of Personal Data to evaluate certain personal aspects relating to an individual, in particular to analyse or predict aspects concerning that individual's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements. Profiling is an example of Automated Processing.

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 Data relating to them.

Data Controller: the person or organisation that determines when, why and how to process Personal Data. It is responsible for establishing practices and policies in line with the Data Protection Legislation. We are the Data Controller of all Personal Data relating to our Personnel and Personal Data used in our business for our own commercial purposes.

Data Privacy Impact Assessment (DPIA): tools and assessments used to identify and reduce high risk data processing activities. DPIA can be carried out as part of Data Protection by Design and Default. DPIA's should be conducted for all major system or business change programs involving the Processing of Personal Data and the circumstances detailed in section 12.4.4.

Data Processor: includes any person or organisation that Processes Personal Data on behalf of a Data Controller and in accordance with the Data Controller's instructions.

Data Protection by Design and Default: implementing appropriate technical and organisational measures in an effective manner to ensure compliance with Data Protection Legislation.

Data Protection Legislation: means the Data Protection Act 2018 (the DPA), the UK General Data Protection Regulation (UK GDPR) and the Privacy and Electronic Communications Regulations 2003 (the PECRs).

Data Protection Manager: means an individual assigned with the responsibility for overseeing our compliance with GDPR.

Data Protection Officer: the person required to be appointed in specific circumstances under the Data Protection Legislation. Where a mandatory Data Protection Officer has not been appointed, this term means an individual voluntarily appointed for this role.

Data Retention Policy: our internal policy which documents the retention periods for Personal Data we hold and the agreed Process for disposal of such Personal Data.

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

EEA: the 27 countries in the EU, and Iceland, Liechtenstein and Norway.

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

Personal Data Breach: any act or omission that compromises the security, confidentiality, integrity or availability of Personal Data or the physical, technical, administrative or organisational safeguards that we or our third-party service providers put in place to protect it, for example:

- loss or theft of data or equipment on which personal information is stored;
- unauthorised access to or use of personal information either by a member of staff or third party;
- loss of data resulting from an equipment or systems (including hardware and software) failure;
- human error, such as accidental deletion or alteration of data;
- unforeseen circumstances, such as a fire or flood; deliberate attacks on IT systems, such as hacking, viruses or phishing scams; and
- 'blagging' offences, where information is obtained by deceiving the organisation which holds it.

Privacy Notices: separate notices setting out information that may be provided to Data Subjects when the Organisation collects information about them. These notices may take the form of general privacy statements applicable to a specific group of individuals (for example, employee privacy notices or customer privacy notices which refer to a long privacy policy) or they may be stand alone, one time privacy statements covering Processing related to a specific purpose.

Privacy Policy: the Organisation's privacy policy which provides more detailed information how it Processes Personal Data often cross referred to

in a privacy notice and available on the Organisation's website (or if an employee the privacy policy available in the staff handbook).

Processing, Process or Processed: any activity that involves the use of Personal Data. 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 Data 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.

Related Policies: the Organisation's policies, operating procedures or processes relating to data protection.

Staff Privacy Policy: our internal privacy policy which details how we use employees, workers, contractors, agency workers, consultants, directors, members and other related individuals' Personal Data.

4. PERSONAL DATA PROTECTION PRINCIPLES

4.1 We adhere to the principles relating to Processing of Personal Data set out in the UK GDPR which require Personal Data to be:

4.1.1 Processed lawfully, fairly and in a transparent manner **(Lawfulness, Fairness and Transparency)**.

4.1.2 Collected only for specified, explicit and legitimate purposes **(Purpose Limitation).**

4.1.3 Adequate, relevant and limited to what is necessary in relation to the purposes for which it is Processed **(Data Minimisation)**.

4.1.4 Accurate and where necessary kept up to date **(Accuracy)**.

4.1.5 Not kept in a form which permits identification of Data Subjects for longer than is necessary for the purposes for which the data is Processed **(Storage Limitation)**.

4.1.6 Processed in a manner that ensures its security using appropriate technical and organisational measures to protect against unauthorised or unlawful Processing and against accidental loss, destruction or damage **(Security, Integrity and Confidentiality)**.

4.2 We are responsible for and must be able to demonstrate compliance with the data protection principles listed above **(Accountability)**.

5. LAWFULNESS, FAIRNESS, TRANSPARENCY

5.1 Lawfulness And Fairness

Basis for processing Personal Data

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

5.1.2 You may only collect, Process and share Personal Data fairly and lawfully and for specified purposes. Data Protection Legislation restricts our actions regarding Personal Data to specified lawful purposes. These restrictions are not intended to prevent Processing, but ensure that we Process Personal Data fairly and without adversely affecting the Data Subject.

5.1.3 Data Protection Legislation allows Processing for specific purposes, some of which are set out below:

5.1.3.1 the Data Subject has given his or her Consent;

5.1.3.2 the Processing is necessary for the performance of a contract with the Data Subject;

5.1.3.3 to meet our legal compliance obligations;

5.1.3.4 to protect the Data Subject's vital interests; or

5.1.3.5 to pursue our legitimate interests for purposes where they are not overridden because the Processing prejudices the interests or fundamental rights and freedoms of Data Subjects. The purposes for which we process Personal Data for legitimate interests needs to be set out in applicable Privacy Notices. If we conduct any new Processing where we rely on this basis, we must normally complete a Legitimate Interest Assessment.

Special Category Data

What is Special Category Data?

Special Category Data is data that is given special protection under data protection law. It includes information revealing racial or ethnic origin, political opinions, religious or similar beliefs, trade union membership, physical or mental health conditions, sexual life, sexual orientation, and biometric or genetic data.

5.1.4 The Organisation may from time to time need to process Special Category Data. We will only process Special Category Data if:

5.1.4.1 we have a lawful basis for doing so, for example because

5.1.4.1.1 the Data Subject has given clear consent;

5.1.4.1.2 the processing is necessary for a contract we have with the individual;

5.1.4.1.3 the processing is necessary for you to comply with the law (not including contractual obligations);

5.1.4.1.4 the processing is necessary to protect someone's life; and

5.1.4.1.5 the processing is necessary for you to perform a task in the public interest or for your official functions, and the task or function has a clear basis in law.

5.1.4.2 one of the special conditions for processing Special Category Data also applies, for example:

5.1.4.2.1 the Data Subject has given explicit consent;

5.1.4.2.2 the processing is necessary for the purposes of exercising the employment law rights or obligations of the Organisation or the Data Subject;

5.1.4.2.3 the processing is necessary to protect the data subject's vital interests, and the Data Subject is physically incapable of giving consent;

5.1.4.2.4 processing relates to personal data which are manifestly made public by the Data Subject;

5.1.4.2.5 the processing is necessary for the establishment, exercise or defence of legal claims; or

5.1.4.2.6 the processing is necessary for reasons of substantial public interest.

5.1.5 Before processing any Special Category Data, staff must notify Data Protection Manager of the proposed Processing, so that they can assess whether the Processing complies with the criteria noted above.

5.1.6 Special Category Data will not be Processed until:

5.1.6.1 the assessment referred to in paragraph 5.1.5 has taken place; and

5.1.6.2 the individual has been properly informed (by way of a Privacy Notice or otherwise) of the nature of the Processing, the purposes for which it is being carried out and the legal basis for it.

5.1.7 Our Privacy Notice sets out the types of Special Category Data that the Organisation processes, what it is used for and the lawful basis for the Processing.

5.1.8 In relation to Special Category Data, the Organisation will comply with the procedures set out in paragraph 5.1.9 and 5.1.10 below to make sure that it complies with the data protection principles set out in paragraph 4 above.

5.1.9 **During the recruitment process:** the HR department, with guidance from Data Protection Manager, will ensure that (except where the law permits otherwise):

5.1.9.1 during the short-listing, interview and decision-making stages, no questions are asked relating to Special Category Data, e.g. race or ethnic origin, trade union membership or health;

5.1.9.2 if Special Category Data is received, e.g. the applicant provides it without being asked for it within his or her CV or during the interview no record is kept of it and any reference to it is immediately deleted or redacted;

5.1.9.3 any completed equal opportunities monitoring form is kept separate from the individual's application form, and not be seen by the person shortlisting, interviewing or making the recruitment decision;

5.1.9.4 'right to work' checks are carried out before an offer of employment is made unconditional, and not during the earlier short-listing, interview or decision-making stages;

5.1.9.5 we will not ask health questions in connection with recruitment and only ask health questions once an offer of employment has been made.

5.1.10 **During employment**: the HR department, with guidance from the Data Protection Manager, will process Personal Data and Special Category Data in accordance with our Staff Privacy Policy.

5.2 CONSENT

5.2.1 A Data Controller must only process Personal Data on the basis of one or more of the lawful bases set out in Data Protection Legislation, which may include Consent.

5.2.2 A Data Subject consents to Processing of their Personal Data if they indicate agreement clearly either by a statement or positive action to the Processing. Consent requires affirmative action so silence, pre-ticked boxes or inactivity are unlikely to be sufficient. If Consent is given in a document which deals with other matters, then the Consent must be kept separate from those other matters.

5.2.3 Data Subjects must be easily able to withdraw Consent to Processing at any time and withdrawal must be promptly honoured. Consent may need to be refreshed if you intend to Process Personal Data for a different and incompatible purpose which was not disclosed when the Data Subject first consented.

5.2.4 Usually we will be relying on another legal basis (and not require Explicit Consent) to Process most types of Special Category Data. Where Explicit Consent is required, you must issue a Privacy Notice to the Data Subject to capture Explicit Consent. You will need to evidence Consent captured and keep records of all Consents so that the Organisation can demonstrate compliance with Consent requirements.

5.3 TRANSPARENCY (NOTIFYING DATA SUBJECTS)

5.3.1 Data Protection Legislation requires Data Controllers 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.

5.3.2 Whenever we collect Personal Data directly from Data Subjects, including for human resources or employment purposes, we must provide the Data Subject with all the information required by Data Protection Legislation including but not limited to the identity of the Data Controller and Data Protection Manager, how and why we will use, Process, disclose, protect and retain that Personal Data through a Privacy Notice which must be presented when the Data Subject first provides the Personal Data.

5.3.3 When Personal Data 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 Data Protection Legislation as soon as possible after collecting/receiving the data. You must also check that the Personal Data was collected by the third party in accordance with Data Protection Legislation and on a basis which contemplates our proposed Processing of that Personal Data.

6. DATA SUBJECT'S RIGHTS AND REQUESTS

6.1 Data Subjects have rights when it comes to how we handle their Personal Data. These include rights to:

6.1.1 to be informed about how, why and on what basis their Personal Data is being processed (Privacy Notice):

6.1.2 withdraw Consent to Processing at any time;

6.1.3 request access to their Personal Data that we hold;

6.1.4 prevent our use of their Personal Data for direct marketing purposes;

6.1.5 ask us to erase Personal Data if it is no longer necessary in relation to the purposes for which it was collected or Processed or to rectify inaccurate data or to complete incomplete data;

6.1.6 restrict Processing in specific circumstances;

6.1.7 challenge Processing which has been justified on the basis of our legitimate interests or in the public interest;

6.1.8 object to decisions based solely on Automated Processing, including profiling (ADM);

6.1.9 prevent Processing that is likely to cause damage or distress to the Data Subject or anyone else;

6.1.10 be notified of a Personal Data Breach which is likely to result in high risk to their rights and freedoms;

6.1.11 make a complaint to the supervisory authority (often the Information Commissioner's Office); and

6.1.12 in limited circumstances, receive or ask for their Personal Data to be transferred to a third party in a structured, commonly used and machine readable format (often referred to as Data Portability).

6.2 Before responding to a request regarding any of the rights listed above, True North will normally need to verify the identity of the individual making the request (to avoid disclosing personal data to a third party without proper authorisation). True North will usually engage an external data protection specialist to assist with this process and to advise on how to respond. If you receive a request like this, you should notify Norma Wiznevitz immediately so legal advice can be sought in a timely manner.

7. PURPOSE LIMITATION

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

7.2 You cannot use Personal Data 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 or where an exemption applies e.g. where further processing is undertaken for archiving purposes in the public interest, for scientific or historical research purposes or for statistical purposes.

8. DATA MINIMISATION

8.1 Personal Data must be adequate, relevant and limited to what is necessary in relation to the purposes for which it is Processed.

8.2 You may only collect Personal Data that you require for your job duties: do not collect excessive data. Ensure any Personal Data collected is adequate and relevant for the intended purposes and that you only Process Personal Data when performing your job duties which require it.

8.3 You must ensure that when Personal Data is no longer needed for specified purposes, it is deleted or anonymised in accordance with the Organisation's Data Retention Policy.

9. ACCURACY

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

9.2 You will ensure that the Personal Data 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 Data at the point of collection and at regular intervals afterwards and take all reasonable steps to destroy or amend inaccurate or out-of-date Personal Data. In terms of your own Personal Data, you should let the HR team know if the information you have provided to us charges, for example, if you move house or change details of the bank or building society account to which you are paid.

10. STORAGE LIMITATION

10.1 Personal Data must not be kept in an identifiable form for longer than is necessary for the purposes for which the data is Processed.

10.2 You must not keep Personal Data 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.

10.3 The Organisation has created a Data Retention Policy which is designed to enable employees to identify for how long Personal Data will normally be held and when it will normally be deleted.

10.4 You will take all reasonable steps to destroy or erase from our systems all Personal Data that we no longer require in accordance with the Organisation's Data Retention Policy. This includes requiring third parties to delete such data where applicable.

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

11. SECURITY INTEGRITY AND CONFIDENTIALITY

11.1 Protecting Personal Data

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

11.1.2 We will develop, implement and maintain safeguards appropriate to our size, scope and business, our available resources, the amount of Personal Data that we own or maintain on behalf of others and identified risks (including use of encryption and Pseudonymisation where applicable) in accordance with the Organisation's policies and procedures relating to information security as may be from time to time in place. We will regularly evaluate and test the effectiveness

of those safeguards to ensure security of our Processing of Personal Data. Technical and organisational measures may include:

11.1.2.1 making sure that, where possible, personal information is pseudonymised or encrypted;

11.1.2.2 ensuring the ongoing confidentiality, integrity, availability and resilience of processing systems and services;

11.1.2.3 ensuring that, in the event of a physical or technical incident, availability and access to personal information can be restored in a timely manner; and

11.1.2.4 a process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing.

11.1.3 Where we use external organisations to process personal information on our behalf, we will implement additional security arrangements in contracts with those organisations to safeguard the security of personal information we hold. If you are engaging a third party to Process Personal Data on the Organisation's behalf, you must first contact the Data Protection Manager to ensure contractual safeguards are in place. In particular, the contracts with external organisations must provide that:

11.1.3.1 The external organisation may only act on our written instructions;

11.1.3.2 Appropriate measures are taken to ensure security of any processing;

11.1.3.3 Sub-contractors are only engaged with our prior consent and under written contract;

11.1.3.4 External organisations are subject to confidentiality requirements;

11.1.3.5 The external organisation will assist us in meeting our obligations in relation to security of processing, notification of data breaches and data protection impact assessment; and

11.1.3.6 The external organisation agrees to undergo audits and inspections, to provide us with information we request to ensure we are meeting our data protection obligations and to tell us immediately if

it is asked to do something which infringes Data Protection Legislation.

11.1.4 You are responsible for protecting the Personal Data we hold. You must implement reasonable and appropriate security measures against unlawful or unauthorised Processing of Personal Data and against the accidental loss of, or damage to, Personal Data. You must exercise particular care in protecting Special Category Data from loss and unauthorised access, use or disclosure and you must follow all procedures and technologies we put in place to maintain the security of all Personal Data from the point of collection to the point of destruction.

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

11.1.5.1 Confidentiality means that only people who have a need to know and are authorised to use the Personal Data can access it.

11.1.5.2 Integrity means that Personal Data is accurate and suitable for the purpose for which it is Processed.

11.1.5.3 Availability means that authorised users are able to access the Personal Data when they need it for authorised purposes.

11.2 Security Procedures

Adequate security procedures should be put in place which include:

11.2.1 **Entry controls:** Any stranger seen in entry-controlled areas should be reported.

11.2.2 **Secure lockable desks and cupboards:** Desks and cupboards should be kept locked if they hold confidential information of any kind. (Personal information is always considered confidential.)

11.2.3 **Methods of disposal:** Paper documents should be shredded. Floppy disks and CD-ROMs should be physically destroyed when they are no longer required.

11.2.4 **Equipment:** Data users should ensure that individual monitors do not show confidential information to passers-by and that they log off from their PC when it is left unattended. All computers should be turned off overnight.

11.2.5 **Password protection and encryption:** Only those who need to access personal data should be able to access it.

11.2.6 **Restricted Circulation:** All production personnel should be briefed to ensure that they restrict circulation of any production paperwork, call sheets, release forms etc. both within and outside the office.

11.2.7 **Vimeo and Wetransfer:** All video uploads must be password protected. The links must be sent on a different email to the password and the passwords should be unique for that particular upload. Passwords will be generated by the edit assistants. Also, all video uploads should be available for a limited length of time – generally two weeks.

11.2.8 **Email Communications:** When sending a mass email using personal email addresses, care should be taken to use the 'blind copy'. This should be using the IT approved mail out function and must be referred to Norma Wisnevitz in advance for approval before sending the email and double checked before pressing send.

11.2.9 **Copy Documents:** Staff should not make unnecessary paper or electronic copies of documentation containing personal information. Copies of documents should not be left at the photocopier, scanner or fax machine.

11.2.10 **Police Requests:** When a request for information is received from the Police we may be compelled to provide the information. The request should immediately be passed to the relevant Executive Producer or to the Data Protection Manager Norma Wisnevitz to deal with. We will also consult with the relevant Commissioning Editor before any disclosure on information relating to programme materials or rushes, as there may be legitimate legal and editorial grounds for resisting disclosure.

11.2.11 **Production Closedown:** On closedown of a production the Data Protection Manager Norma Wisnevitz and Executive Producer should review what personal data records can be legitimately retained or destroyed.

11.2.12 **Telephone Disclosure:** Any member of staff dealing with telephone enquiries should be careful about disclosing any personal information held by us. In particular they should:

- Check the caller's identity to make sure that information is only given to a person who is entitled to it.
- Suggest that the caller put their request in writing if they are not sure about the caller's identity and where their identity cannot be checked.

- Refer to their line manager or Data Protection Manager Norma Wisnevitz for assistance in difficult situations. No-one should be bullied into disclosing personal information.

11.2 **Sharing Personal Data**

11.2.1 We are required to comply with obligations under Data Protection Legislation where we use third parties to process Personal Data on our behalf (including but not limited to IT software providers and HR payroll providers). In these circumstances, such parties will be acting as our Data Processor and Data Protection Legislation requires us to put in place a contract in writing which contains a number of provisions to help safeguard the Personal Data. If you are responsible for the drafting or negotiation of contracts with Data Processors, you must seek further advice from the Data Protection Manager to ensure the contracts contain all the necessary data protection provisions.

11.2.2 Where we share Personal Data with third parties for their own use (and they will not be processing data on our behalf) it will often be necessary to enter into a data sharing agreement. We need to ensure that such agreements contain certain provisions such as the third party will only process the Personal Data for specific purposes, to return the Personal Data to us in certain circumstances and have adequate security measures in place.

11.2.3 In all cases, we may only share the Personal Data we hold provided the sharing complies with the Privacy Notice/Privacy Policy provided to the Data Subject.

11.3 **Reporting A Personal Data Breach**

11.3.1 Data Protection Legislation requires Data Controllers to notify a Personal Data Breach to the applicable regulator within 72 hours of becoming aware of the breach where the breach is likely to result in a risk to the rights and freedom of individuals. It will also be necessary to inform the Data Subject when a breach occurs which is likely to be a high risk to the rights and freedom of the Data Subject.

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

11.3.3 If you know or suspect that a Personal Data Breach has occurred, do not attempt to investigate the matter yourself. Immediately notify the Data Protection Manager. An internal

record of any data breach must also be made. You should preserve all evidence relating to the potential Personal Data Breach.

11.3.4 Where we act as Data Processor for a third party, we must make the Data Controller aware of the Personal Data Breach as soon as possible.

11.4 **Transfer Limitation**

11.4.1 Data Protection Legislation restricts data transfers to countries outside the UK in order to ensure that the level of data protection afforded to individuals by Data Protection Legislation is not undermined. You may only transfer Personal Data outside the UK if one of the following conditions applies:

11.4.1.1 the Information Commissioners Office (ICO) has issued a decision confirming that the country to which we transfer the Personal Data ensures an adequate level of protection for the Data Subjects' rights and freedoms, please see the ICO website for details of those countries; or

11.4.1.2 appropriate safeguards are in place such as UK binding corporate rules (UK BCR), standard contractual clauses approved under UK GDPR (the International Data Transfer Agreement and Addendum), an approved code of conduct or a certification mechanism, contractual clauses authorised by the ICO.

12. **ACCOUNTABILITY**

12.1 The Data Controller must implement appropriate technical and organisational measures in an effective manner, to ensure compliance with data protection principles. The Data Controller is responsible for, and must be able to demonstrate, compliance with the data protection principles.

12.1.1 The Organisation must have adequate resources and controls in place to ensure and to document Data Protection Legislation compliance including:

12.1.1.1 appointing a suitably qualified Data Protection Officer (where necessary). Where the appointment of a Data Protection Officer is not a legal requirement we must still appoint an individual/individuals with responsibility for overseeing our compliance with Data Protection Legislation such as a Data Protection Manager;

12.1.1.2 implementing Data Protection by Design and Default when Processing Personal Data and completing DPIAs where Processing presents a high risk to rights and freedoms of Data Subjects;

12.1.1.3 integrating data protection into internal documents including this Data Protection Policy, Related Policies and Privacy Notices;

12.1.1.4 regularly training Organisation Personnel on Data Protection Legislation, this Data Protection Policy, Related Policies and data protection matters including, for example, Data Subject's rights, Consent, legal basis, DPIA and Personal Data Breaches, with such training to normally be offered once every year. The Organisation must maintain a record of training attendance by Organisation Personnel; and

12.1.1.5 regularly testing the privacy measures implemented and conducting periodic reviews and audits to assess compliance, including using results of testing to demonstrate compliance improvement effort.

12.2 **Record Keeping**

12.2.1 Data Protection Legislation requires us to keep full and accurate records of all our data Processing activities.

12.2.2 You must keep and maintain accurate corporate records reflecting our Processing including records of Data Subjects' Consents.

12.2.3 We must also keep records of the name and contact details of the Data Controller and the Data Protection Manager, clear descriptions of the Personal Data types, Data Subject types, Processing activities, Processing purposes, third-party recipients of the Personal Data, Personal Data transfers outside the EEA and the safeguards put in place to protect the transfer of such Personal Data, the Personal Data's retention period and a description of the security measures in place.

12.2.4 If we process Special Category Data and criminal records information, we will also keep written records of:

12.2.4.1 the relevant purpose for which the processing takes place, including (where required) why it is necessary for that purpose;

12.2.4.2 the lawful basis for our processing; and

12.2.4.3 whether we retain and erase the personal information in accordance with our policy document and, if no, the reasons for not following our policy.

12.2.5 Please see ICO guidance for further details regarding the information you must record:https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/accountability-and-governance/documentation/

12.2.6 We will conduct regular reviews of the personal information we process and update our documentation according. This may include:

12.2.6.1 carrying out information audits to find out what Personal Data the Organisation holds;

12.2.6.2 distributing questionnaires and talking to staff across the Organisation to get a more complete picture of our Processing activities; and

12.2.6.3 reviewing our policies, procedures, contract and agreements to address areas such as retention, security and data sharing.

12.3 **Training And Audit**

12.3.1 We are required to ensure all Organisation Personnel have undergone adequate training to enable them to comply with data privacy laws. We must also regularly test our systems and processes to assess compliance.

12.3.2 You must regularly review all the systems and processes under your control to ensure they comply with this Data Protection Policy and check that adequate governance controls and resources are in place to ensure proper use and protection of Personal Data.

12.4 **Data Protection By Design and Default And Data Protection Impact Assessment (DPIA)**

Data Protection by Design and Default

12.4.1 We are required to implement Data Protection by Design and Default measures when Processing Personal Data. This means that we must implement appropriate technical and organisational measures (like Pseudonymisation) and appropriate safeguards into every aspect of our processing activities in an effective manner, from the design stage of any process, service, system or product and regularly

throughout its lifecycle to ensure compliance with data privacy principles.

12.4.2 You must assess what Data Protection by Design and Default measures can be implemented on all programs/systems/processes that Process Personal Data by taking into account the following:

12.4.2.1 the cost of implementation;

12.4.2.2 the nature, scope, context and purposes of Processing; and

12.4.2.3 the risks of varying likelihood and severity for rights and freedoms of Data Subjects posed by the Processing.

DPIA's

12.4.3 Data Controllers must also conduct DPIAs in respect to high risk Processing.

12.4.4 You should conduct a DPIA (and discuss your findings with the Data Protection Manager) when implementing system or business change programs involving the Processing of Personal Data including:

12.4.4.1 use of new technologies (programs, systems or processes), or changing technologies (programs, systems or processes);

12.4.4.2 Automated Processing including profiling and ADM which have legal or similarly significant effect on Data Subjects;

12.4.4.3 large scale Processing of Special Category Data; and

12.4.4.4 large scale, systematic monitoring of a publicly accessible area.

12.4.5 A DPIA must include:

12.4.5.1 a description of the Processing, its purposes and the Data Controller's legitimate interests if appropriate;

12.4.5.2 an assessment of the necessity and proportionality of the Processing in relation to its purpose;

12.4.5.3 an assessment of the risk to individuals; and

12.4.5.4 the risk mitigation measures in place and demonstration of compliance.

If you think you may need to complete a DPIA, True North will normally engage an external data protection specialist to advise further and assist with that process.

If you think you may need to do this, please contact Norma Wisnevitz.

See ICO guidance for further information on how to undertake DPIA's (https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/accountability-and-governance/data-protection-impact-assessments/)

12.5 **Automated Processing (Including Profiling) And Automated Decision-Making (ADM)**

12.5.1 Generally, ADM is prohibited when a decision has a legal or similar significant effect on an individual unless:

12.5.1.1 a Data Subject has Explicitly Consented;

12.5.1.2 the Processing is authorised by law; or

12.5.1.3 the Processing is necessary for the performance of or entering into a contract.

12.5.2 If a decision is to be based solely on Automated Processing (including profiling), then Data Subjects must be informed when you first communicate with them of their right to object.

12.5.3 We must also inform the Data Subject of the logic involved in the decision making or profiling, the significance and envisaged consequences and give the Data Subject the right to request human intervention, express their point of view or challenge the decision.

12.5.4 A DPIA must be carried out before any Automated Processing (including profiling) or ADM activities are undertaken which has a legal effect or similar significant effect on the Data Subject. Note that not all Authorised Processing will have a legal or similar effect on a Data Subject, for example, targeted advertising is generally not considered to have a significant effect on individuals.

13. DIRECT MARKETING

13.1 We are subject to certain rules and privacy laws when marketing to our customers.

13.2 For example, a Data Subject's prior consent is required for electronic direct marketing (for example, by email, text or automated calls). The limited exception for existing customers known as "soft opt in" allows organisations to send marketing texts or emails if they have

obtained contact details in the course of a sale to that person, they are marketing similar products or services, and they gave the person an opportunity to opt out of marketing when first collecting the details and in every subsequent message.

13.3 The right to object to direct marketing must be explicitly offered to the Data Subject in an intelligible manner so that it is clearly distinguishable from other information.

13.4 A Data Subject's objection to direct marketing must be promptly honoured. If a customer opts out at any time, their details should be suppressed as soon as possible. Suppression involves retaining just enough information to ensure that marketing preferences are respected in the future.

14. CHANGES TO THIS DATA PROTECTION POLICY

14.1 We reserve the right to change this Data Protection Policy at any time without notice to you so please check back regularly to obtain the latest copy of this Data Protection Policy. We last revised this Data Protection Policy in March 2025.

14.2 This Data Protection Policy does not override any applicable national data privacy laws and regulations in countries where the Organisation operates.