

Yeti Media Ltd

DATA PROTECTION POLICY

1. Introduction

Yeti holds personal data about job applicants, employees, workers, viewers, suppliers and other individuals for a variety of purposes.

Yeti recognises that the correct and lawful treatment of personal data will maintain confidence in the organisation and will provide for successful operations. Protecting the confidentiality and integrity of personal data is a critical responsibility that we take seriously at all times.

This policy sets out how Yeti seeks to protect personal data and ensure staff understand the rules governing their use of personal data to which they have access in the course of their work.

This policy applies to all personal data Yeti processes regardless of the media on which that data is stored or whether it relates to past or present employees, workers, viewers, suppliers or any other individuals.

This policy requires staff to ensure that the DATA PROTECTION OFFICER is consulted before any significant new data processing activity is initiated to ensure that relevant compliance steps are addressed.

The Data Protection Officer is responsible for the monitoring and implementation of this policy. If you have any questions about the content of this policy or other comments you should contact the Data Protection Officer. In particular, staff **must always** contact the Data Protection Officer in the following circumstances:

It is unclear which lawful basis should be relied upon to process personal data (including the legitimate interests used by Yeti (see section below);

It is necessary to rely on the consent and/or explicit consent to process personal data (see section below);

It is necessary to draft a privacy notice (see section below);

If the retention period for the personal data being processed is unclear or unknown (see section below);

It is unclear what security or other measures need to be implemented to protect personal data (see section below);

Personal data is being transferred outside the EEA (see section below);

If there has been a personal data breach (section below);

Whenever there is a significant change in processing activity or new processing activity in relation to personal data (this may require a Data Protection Impact Assessment) (see section below);

It is intended that personal data will be used for a purpose other than what it was collected for;

If activities involving automated processing including profiling or automated decision-making are planned (see section below).

2. Scope

3. 2.1 This policy applies to all staff, which for these purposes includes employees, temporary and agency workers, other contractors, interns and volunteers.

4. 2.2 All staff must be familiar with this policy and comply with its terms.

5. 2.3 Compliance with this policy is mandatory. Staff must also comply with any related policies and privacy notices. Any breach of this Data Protection Policy may result in disciplinary action

6. 2.4 Yeti may supplement or amend this policy by additional policies and guidelines from time to time.

7. Definitions

3.1 In this policy:

(a) **Personal data** means information relating to identifiable individuals, such as job applicants, current and former employees, agency, contract and other staff, viewers, suppliers and marketing contacts. This includes expression of opinion about the individual and any indication of someone else's intentions towards the individual.

(b) **Special category personal data** means 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. Personal data relating to criminal offences and convictions should also be treated as special category personal data.

(c) **Processing data** 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.

8. General principles

4.1 Yeti's policy is to process personal data in accordance with the applicable data protection laws and rights of individuals as set out below. All staff have personal responsibility for the practical application of Yeti's Data Protection Policy.

4.2 Yeti will observe the following principles in respect of the processing of personal data, ensuring that personal data is:

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

(b) Collected only for specified, explicit and legitimate purposes ('Purpose Limitation').

(c) Adequate, relevant and limited to what is necessary in relation to the purposes for which it is processed ('Data Minimisation').

(d) Accurate and where necessary kept up to date ('Accuracy').

(e) Not kept in a form which permits identification of individuals for longer than is necessary for the purposes for which the data is processed ('Storage Limitation').

(f) 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').

4.3 Yeti is responsible for and must be able to demonstrate compliance with the data protection principles listed above (the 'Principle of Accountability').

9. Lawfulness, Fairness and Transparency

5.1 Personal data must be processed lawfully, fairly and in a transparent manner in relation to the individual.

Lawfulness

5.2 Staff should ensure that there is a legal basis for processing personal data. The legal bases for processing are as follows:

(g) the individual has given his or her consent (see below);

(h) the processing is necessary for the performance of a contract with the individual;

(i) to meet Yeti's legal compliance obligations;

(j) to protect the individual's vital interests;

(k) for the performance of a task in the public interest;

(l) to pursue Yeti's legitimate interests, where these interests are not overridden because the processing prejudices the interests or fundamental rights and freedoms of the individual(s). The purposes for which we process personal data for legitimate interests need to be set out the privacy notices (see section below).

5.3 If staff are unsure what legal basis is applicable to the personal data they are processing they should contact the Data Protection Officer.

5.4 Special category personal data (see above) requires higher levels of protection and a further legal basis in addition to those outlined in section 5.2 above for processing to be lawful.

5.5 The *explicit* consent of the individual will normally be the appropriate additional legal basis for processing special category personal data in relation to viewers or members of the public. Staff should contact the Data Protection Officer for more information the appropriate legal basis for processing special category data.

5.6 Yeti will also be processing special category personal data in relation to its staff. The additional legal basis for processing the special category personal data of staff will ordinarily be that it is necessary for the purposes of carrying out the obligations and exercising specific rights in the field of employment law or that the processing is necessary for reasons of substantial public interest, for example monitoring equality, preventing or detecting unlawful acts, protecting the public against dishonesty, safeguarding, preventing fraud or suspicion of terrorism or money laundering. Staff should contact the Data Protection Officer for more information on the appropriate legal basis for processing special category personal data. In addition, staff should pay particular attention to section 12 below.

Fairness & Transparency (Privacy Notices)

5.7 Data protection law requires us to provide detailed, specific information to individuals about how and why their personal data is being processed. Such information must be provided through appropriate privacy notices.

5.8 Privacy notices must be concise, transparent, intelligible, easily accessible, and in clear and plain language so that an individual can easily understand them.

5.9 Whenever Yeti collects personal data directly from an individual, the individual must be provided with a privacy notice containing all the information required by data protection law (including the identity of the data controller and the Data Protection Officer, how and why Yeti will use, process, disclose, protect and retain that personal data). The privacy notice will also make it clear what legal basis is being relied upon and the additional appropriate

legal basis if special category personal data is being processed. The privacy notice must be provided when the individual first provides Yeti with the personal data. Yeti's general privacy notice will usually be appropriate in relation to the general purposes for which Yeti collects personal data. Staff should direct the individual to this privacy notice at the point that the personal data is collected. This is available here: www.yetitelevision.com

5.10 When personal data is collected indirectly (for example, from a third party or publicly available source), the individual must be provided with a privacy notice including all the information required under data protection law, as soon as possible, after collecting/receiving the data, but no later than the first communication with the individual or 1 month from receiving the personal data (whichever is earlier), unless this proves impossible or would involve disproportionate effort. As in above Yeti's general privacy notice will usually be appropriate in relation to the general purposes for which Yeti collects personal data. Staff should direct the individual to this privacy notice in the first communication or within 1 month of receiving the personal data, whichever is earlier. This is available here: www.yetitelevision.com Staff should inform the Data Protection Officer, if this is likely to prove impossible or involve disproportionate effort.

5.11 Staff must also check that the personal data was collected by the third party in accordance with data protection law and on a basis which contemplates Yeti's proposed processing of that personal data.

5.12 Staff should contact the Data Protection Officer if it is necessary to draft a privacy notice or if they are unclear as to when a privacy notice is required.

10. Purpose limitation

6.1 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.

6.2 Staff cannot use personal data for new, different or incompatible purposes from those disclosed when the personal data was first obtained, unless staff have informed the individuals of the new purposes and legal basis being relied upon (if this legal basis is consent, appropriate consent must be obtained (see section below).

11. Data minimisation

7.1 Personal data must be adequate, relevant and limited to what is necessary in relation to the purposes for which it is processed.

7.2 Staff may only process personal data when performing job duties requires. Excessive personal data should not be collected and staff should ensure, to the best of their abilities, that any personal data collected is adequate and relevant for the intended purposes.

7.3 Staff must ensure that when personal data is no longer needed for specified purposes, it is deleted or anonymised. in accordance with Yeti's Data Retention Policy.

12. Accuracy

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

8.2 Staff will ensure that the personal data Yeti uses and holds is accurate, complete, kept up to date and relevant to the purpose for which we collected it. Staff must check the accuracy of any personal data at the point of collection and at regular intervals afterwards. Staff must take all reasonable steps to destroy or amend inaccurate or out-of-date personal data.

8.3 Staff must ensure that personal data held by Yeti relating to them is accurate and updated as required. If personal details or circumstances change, staff should inform the HR DEPARTMENT, so Yeti's records can be updated.

13. Storage limitation (data retention)

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

9.2 Staff must not keep personal data, in a form which permits the identification of an individual, for longer than needed for the legitimate purpose or purposes for which Yeti originally collected it.

9.3 Yeti maintains a Data Retention Policy to ensure personal data is deleted, after a reasonable time, when it is no longer required for the purposes for which it was being held.

9.4 Staff will take all reasonable steps to destroy or erase from Yeti's systems all personal data that we no longer require. in accordance with Yeti's Data Retention Policy. This includes requiring third parties to delete such data where applicable.

9.5 Staff will ensure individuals are informed of the period for which data is stored and how that period is determined in any applicable privacy notice (see 5.7 - 5.12).

14. Security integrity and confidentiality

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

10.2 Yeti must implement reasonable and appropriate security measures against unlawful or unauthorised processing of personal data and against the accidental loss of, or damage to, or destruction of personal data.

10.3 Yeti must maintain data security by protecting the confidentiality, integrity and availability of the personal data, defined as follows:

(a) Confidentiality means that only people who have a need to know and are authorised to use the personal data can access it.

(b) Integrity means that personal data is accurate and suitable for the purpose for which it is processed.

(c) Availability means that authorised users are able to access the personal data when they need it for authorised purposes.

10.4 Yeti will develop, implement and maintain safeguards appropriate to:

(a) our size, scope and business;

(b) our available resources;

(c) the amount of personal data that we own or maintain on behalf of others; and

(d) identified risks (including use of encryption and pseudonymisation (i.e. 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) where applicable).

10.5 Yeti will regularly evaluate and test the effectiveness of those safeguards to ensure security of our processing of personal data.

10.6 Staff have a responsibility for protecting the personal data Yeti holds.

10.7 Staff must exercise particular care in protecting special category personal data (see above) from loss and unauthorised access, use or disclosure.

10.8 Staff must follow all procedures of Yeti put in place to maintain the security of all personal data from the point of collection to the point of destruction. Staff may only transfer personal data 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 (see sections 15 and below).

10.9 Staff must comply with and not attempt to circumvent the administrative, physical and technical safeguards implemented and maintained in accordance with data protection law and relevant standards to protect personal data.

15. Accountability

11.1 Yeti must implement appropriate technical and organisational measures to ensure compliance with data protection principles (set out in above). Yeti is responsible for, and must be able to demonstrate, compliance with the data protection principles.

11.2 Yeti must have adequate resources and controls in place to ensure and to document data protection law compliance including:

(a) appointing a suitably qualified Data Protection Officer;

(b) implementing data protection by design and default when processing personal data to ensure compliance with applicable data protection laws (see section below);

(c) completing Data Protection Impact Assessments (DPIAs) to identify and reduce risks of a data processing activity, where processing presents a high risk to rights and freedoms of individuals. DPIAs should be conducted for all major system or business change programs involving the processing of personal data particularly those involving new initiatives or technology (see section below);

(d) integrating data protection into internal documents, policies and procedures including this Data Protection Policy;

(e) regularly training staff on applicable data protection law, this Data Protection Policy, related policies and data protection matters including, for example, individual rights, consent, legal basis, DPIAs and personal data breaches; and

(f) 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.

16. Special Category Personal Data

12.1 Because of the particular sensitivities around the processing of special category personal data, the Data Protection Act 2018 ('DPA 2018') requires Yeti to have in place policy documentation to explain Yeti's procedures for securing compliance with the data protection principles (see section 4.2) and explains Yeti's policies as regards the retention and erasure of the special category personal data (section 9 above).

12.2 Accordingly, when processing special category personal data, in addition to the matters set out in sections 5-11 above, consideration must also be given to the matters set out below.

Staff Special Category Personal Data

12.3 When processing staff special category personal data, either in reliance on the legal basis that the processing is necessary for the purposes of carrying out the obligations and exercising specific rights in the field of employment law or in reliance on the substantial public interest ground, particular consideration must be given to:

(a) ensuring that the special category personal data is only shared internally with individuals who need to know the information. This will usually be the HR department and the staff member's line manager. Careful consideration should be given to any further internal sharing and the guidance of the Data Protection Officer sought;

(b) whether it is feasible to anonymise the data, for example when processing special category personal data for equal opportunities monitoring;

(c) the extent of the special category personal data retained

(d) Yeti's Data Retention Policy, as some special category personal data will have specific shorter retention periods, particular care should be taken to ensure that the retention periods specified for such data in Yeti's Data Retention Policy are adhered to.

17. Privacy by Design and Data Protection Impact Assessment (DPIA)

13.1 Yeti is required to implement privacy by design when processing personal data by implementing appropriate technical and organisational measures in an effective manner, to ensure compliance with data privacy principles.

13.2 Yeti must assess what privacy by design measures can be implemented on all programs/systems/processes that process personal data by taking into account the following:

(a) the state of the art (i.e. the highest level of general development, as of a device, procedure, process or technique achieved at the particular time);

(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 individuals posed by the processing.

13.3 Yeti must conduct DPIAs in respect of processing which is considered to be high risk (for example where processing involves special category personal data on a large scale).

13.4 Staff should contact the Data Protection Officer and conduct a DPIA when implementing major system or business change programs involving the processing of personal data including:

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

(b) automated processing including profiling and automated decision making;

(c) large scale processing of special category data; and

(d) large scale, systematic monitoring of a publicly accessible area (e.g. under CCTV).

13.5 A DPIA must include:

(a) a description of the processing, its purposes and the data controller's legitimate interests if appropriate;

(b) an assessment of the necessity and proportionality of the processing in relation to its purpose;

(c) an assessment of the risk to individuals; and

(d) the risk mitigation measures in place and demonstration of compliance.

18. Consent

14.1 Yeti must ensure personal data is processed on the basis of one or more of the lawful bases set out in above, one of which is consent.

14.2 In order for an individual to validly consent to the processing of their personal data, that consent must be freely given, specific, informed and be an unambiguous indication of the individual's wishes by which they, by a statement or by a clear positive action, signify agreement to the processing of personal data relating to them.

14.3 Consent requires *affirmative* action so silence, pre-ticked boxes or inactivity are not sufficient.

14.4 If consent is given in a document which deals with other matters, then the consent must be kept separate from those other matters.

14.5 Individuals 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 Yeti intends to process personal data for a different and incompatible purpose which was not disclosed when the individual first consented.

14.6 Consent should not be relied upon as the legal basis for processing, if another more appropriate legal basis applies.

14.7 Consent should not usually be relied upon where there is an imbalance in the relationship between the individual and Yeti for example in the context of an employer/employee relationship.

14.8 Explicit consent is usually required for:

(a) Processing special category personal data (although staff should contact the Data Protection Officer to determine the most appropriate legal basis for processing special category data).

(b) Automated decision-making; and

(c) Cross border data transfers.

14.9 Explicit consent requires a very clear and specific statement of consent from the individual (that is, not just action) and the individual should be provided with detailed information in relation to the specific purpose for which explicit consent it being sought.

14.10 Staff will need keep records of all consents so that Yeti can demonstrate compliance with consent requirements.

19. Limitations on transfers of data

15.1 Data protection law restricts data transfers to countries outside the European Economic Area ('EEA') in order to ensure that the level of data protection afforded to individuals is not undermined. Personal data is transferred from the originating country across borders when it is transmitted, sent, viewed or access in a different country.

15.2 Yeti may only transfer personal data outside the EEA if one of the following conditions applies:

(a) the European Commission has issued a decision confirming that the country to which the personal data is transferred ensures an adequate level of protection for the individuals' rights and freedoms (an 'adequacy decision');

(b) appropriate safeguards are in place such as binding corporate rules (which are standard contractual clauses approved by the European Commission), an approved code of conduct or a certification mechanism;

(c) the individual has provided explicit consent to the proposed transfer after being informed of any potential risks; or

(d) the transfer is necessary for one of the other reasons set out under data protection law including the performance of a contract between Yeti and the individual, reasons of public interest, to establish, exercise or defend legal claims or to protect the vital interests of the individual where the individual is physically or legally incapable of giving consent and, in some limited cases, for Yeti's legitimate interest.

15.3 Staff should contact the Data Protection Officer before transferring personal data outside the EEA to ensure one of the conditions outlined above is satisfied.

20. Sharing Personal Data

16.1 In general Yeti is not allowed to share personal data with third parties unless certain safeguards and contractual arrangements have been put in place.

16.2 Staff may only share the personal data held by Yeti with another employee, agent or representative if the recipient has a job-related need to know the information and the transfer complies with any applicable cross-border transfer restrictions.

16.3 Where Yeti uses external organisations to process personal data on its behalf, additional security arrangements need to be implemented in contracts with those organisations to safeguard the security of personal data.

16.4 Staff should consult the Data Protection Officer to discuss the necessary steps to ensure compliance when setting up any new agreement or altering any existing agreement.

21. Individuals rights and requests

17.1 Individuals have rights when it comes to how Yeti handles their personal data. These include rights to:

(a) receive certain information about Yeti's processing activities in a privacy notice (see section 5.7 above);

(b) request access to their personal data that Yeti holds (via a subject access request) (access);

(c) ask Yeti to erase personal data if it is no longer necessary in relation to the purposes for which it was collected or processed (erasure);

(d) to rectify inaccurate data or to complete incomplete data (rectification);

(e) to restrict processing in specific circumstances (restriction);

(f) 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 (data portability);

(g) withdraw consent to processing at any time;

(h) prevent Yeti's use of their personal data for direct marketing purposes;

(i) to challenge processing which has been justified on the basis of Yeti's legitimate interests or in the public interest;

(j) request a copy of an agreement under which personal data is transferred outside of the EEA;

(k) object to decisions based solely on automated processing (i.e. when a decision is made which is based solely on automated processing (including profiling) which produces legal effects or significantly affects an individual);

(l) prevent processing that is likely to cause damage or distress to the individual or anyone else;

(m) be notified of a personal data breach which is likely to result in high risk to their rights and freedoms; and

(n) make a complaint to the supervisory authority;

17.2 Staff must immediately forward any request received in relation to the rights outlined above to the Data Protection Officer immediately in accordance with Yeti's Subject Access Request Policy and Individual Rights Policy. This is

particularly important because Yeti must respond to a valid request within the legally prescribed time limits (under GDPR in the majority of circumstances this is 1 month from the day the request is received).

22. Direct marketing

18.1 Yeti is subject to certain rules and privacy laws when marketing to individuals.

18.2 Prior consent is required for electronic direct marketing (for example, by email, text or automated calls). There is a limited exception which Yeti can utilise known as "soft opt in" which allows us to send marketing texts or emails if we have obtained contact details in the course of the provision of services to an individual, we are marketing similar products or services, and we have given the individual an opportunity to opt out of marketing when first collecting the details and in every subsequent communication.

18.3 The right to object to direct marketing (i.e. opt-out or unsubscribe) must be explicitly offered to the individual in an intelligible manner so that it is clearly distinguishable from other information, when their personal data is collected and in every subsequent communication.

18.4 An individual's objection to direct marketing must be promptly honoured. If an individual 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.

23. Automated Processing (including profiling) and Automated Decision-Making

19.1 In general terms automated decision-making is prohibited when a decision has a legal or similar significant effect on an individual unless:

(o) an individual has explicitly consented;

(p) the processing is authorised by law; or

(q) the processing is necessary for the performance of or entering into a contract with the individual.

19.2 If certain types of special category personal data (see) are being processed, then grounds (b) or (c) will not be allowed but such special category personal data can be processed where it is necessary (unless less intrusive means can be used) for substantial public interest like fraud prevention.

19.3 If a decision is to be based solely on automated processing (including profiling), then individuals must be informed that they have the right to object to this in the first communication with them (at the latest). This right must be explicitly brought to their attention and presented clearly and separately from other information. Further, suitable measures must be put in place to safeguard the individual's rights and freedoms and legitimate interests.

19.4 The individual must also be informed in the privacy notice (see above) of the logic involved in the decision making or profiling, the significance and envisaged consequences. The individual must also be and given the right to request human intervention, express their point of view or challenge the decision.

19.5 Staff must contact the Data Protection Officer and a DPIA must be carried out before any automated processing (including profiling) or automated decision-making activities are undertaken.

24. Reporting a Personal Data Breach

20.1 Data protection law requires Yeti to notify personal data breaches to the relevant supervisory authority (for our purposes, this will usually be the Information Commissioner's Office) and individual data subjects, in certain circumstances.

20.2 Staff should be aware that a personal data breach is any act or omission that compromises the security, confidentiality, integrity or availability of personal data or the physical, technical, administrative or organisational safeguards that Yeti or our third-party service providers put in place to protect it. The loss, or unauthorised access, disclosure or acquisition, of personal data is a personal data breach.

20.3 If staff know or suspect that a personal data breach has occurred, they should not attempt to investigate the matter themselves. Yeti has a Personal Data Breach Reporting Procedure in place. Staff should be familiar with this procedure and immediately contact the Data Protection Officer in the event of a personal data breach in accordance with that procedure.

20.4 Staff should ensure that they preserve all evidence relating to the potential personal data breach.

25. Exemptions

21.1 There are a number of exemptions which are applicable to the provisions of data protection law. Yeti considers that the following exemptions may be applicable to its processing activities:

Journalism, literature or art

21.2 Certain provisions of data protection law will not apply when personal data is being processed with a view to publication in relation to the following:

(a) the purposes of journalism;

(b) artistic purposes; or

(c) literary purposes.

provided Yeti reasonably believes that the publication would in the public interest (taking into account the importance of freedom of expression to the public interest) and that the application of the relevant provisions of data protection law would be incompatible with one of the purposes listed above.

21.3 Yeti must take into consideration the following Codes of Practice in determining whether publication is in the public interest:

(a) BBC Editorial Guidelines;

(b) Ofcom Broadcasting Code;

(c) Editors' Code of Practice.

21.4 The Data Protection Officer must authorise any reliance placed on this exemption.

Research and statistics

21.5 Certain more limited provisions of data protection law will not apply when personal data is being processed for:

(a) scientific or historical research purposes, or

(b) statistical purposes,

21.6 This exemption only applies to the extent that the application of those provisions would prevent or seriously impair the achievement of the purposes in question.

21.7 This exemption only applies to the provisions of data protection law relating to:

(a) Further processing. Further processing for historical research or statistical purposes shall not be considered to be incompatible with the initial purpose for which the personal data was processed;

(b) confirmation of processing, access to data and safeguards for third country transfers (where the results of the of the research or any resulting statistics are not made available in a form which identifies an individual);

(c) the right to rectification;

(d) the right to restriction of processing; and

(e) objections to processing.

21.8 Yeti must still ensure that appropriate safeguards, in the form of technical and organisational measures are in place in relation to the processing of personal data for historical research or statistical purposes, in particular in order to ensure compliance with the principle of data minimisation.

21.9 The Data Protection Officer must authorise any reliance placed on this exemption.

26. Consequences of failing to comply

22.1 Yeti takes compliance with this Data Protection Policy very seriously. Failure to comply puts both staff and Yeti at risk. The importance of this data protection policy means that failure to comply with any requirement may lead to disciplinary action, which may result in dismissal.

22.2 Yeti reserves the right to change this Data Protection Policy at any time without notice. Staff should ensure that have the latest copy of this Data Protection Policy.