DATA PROTECTION POLICY

Paternoster Communications Ltd (herein referred to as "the business") has a data protection policy and a Data Protection Controller (DPC), named as Tom Buchanan

General Statement of the business's Duties and Scope

The business is required to process relevant personal data regarding members of staff, volunteers, and customers as part of its operation and shall take all reasonable steps to do so in accordance with this Policy.

Data Protection Controller

The business has appointed the Founding Partner as the Data Protection Controller (DPC) who will endeavour to ensure that all personal data is processed in compliance with this Policy and the Principles of the Data Protection Act 1998. The Freedom of Information Act 2000 and the Protection of Freedoms Act 2012 are also relevant to parts of this policy. The business recognises The General Data Protection Regulation (GDPR) (Regulation (EU) 2016/679) adopted 27 April 2016, the two-year transition period and the application date of 25 May 2018 and is actively working towards compliance with that directive.

The Principles

The business so far as is reasonably practicable complies with the Data Protection Principles (the Principles) contained in the Data Protection Act to ensure all data is:-

- Fairly and lawfully processed
- Processed for a lawful purpose
- Adequate, relevant and not excessive
- Accurate and up to date
- Not kept for longer than necessary
- Processed in accordance with the data subject's rights
- Secure
- Not transferred to other countries without adequate protection

Definitions

- The business is 'Paternoster Communications Ltd'.
- Data Subject, an individual who is the subject of the personal data.

Personal Data

Personal data covers both facts and opinions about an individual where that data identifies an individual. For example, it includes information necessary for employment such as the member of staff's name and address and details for payment of salary. Personal data may also include sensitive personal data as defined in the Act.

Processing of Personal Data

Consent may be required for the processing of personal data unless processing is necessary for the performance of the contract of employment. Any information which falls under the definition of personal data and is not otherwise exempt, will remain confidential and will only be disclosed to third parties with appropriate consent.

Use of those services indicates acceptance and may grant additional consent as to how the business may process personal data. The business processes some personal data for direct marketing and fund-raising purposes, data subjects have the right to request an opt-out to these activities, which must be respected.

Sensitive Personal Data

The business may, from time to time, be required to process sensitive personal data. Sensitive personal data includes data relating to medical information, gender, religion, race, sexual orientation, trade union membership and criminal records and proceedings.

Rights of Access to Information

Data subjects have the right of access to information held by the business, subject to the provisions of the Data Protection Act 1998 and the Freedom of Information Act 2000. Any data subject wishing to access their personal data should put their request in writing to the DPC. The business will endeavour to respond to any such written requests as soon as is reasonably practicable and in any event, within 40 days for access to records and 21 days to provide a reply to an access to Data Protection Policy Lent 2017 3 information request. The information will be imparted to the data subject as soon as is reasonably possible after it has come to the business's attention and in compliance with the relevant Acts.

Exemptions

Certain data is exempted from the provisions of the Data Protection Act which includes the following:-

- National security and the prevention or detection of crime
- The assessment of any tax or duty
- Where the processing is necessary to exercise a right or obligation conferred or imposed by law upon the business, including Safeguarding and prevention of terrorism and radicalisation

The above are examples only of some of the exemptions under the Act. Any further information on exemptions should be sought from the DPC.

Accuracy

The business will endeavour to ensure that all personal data held in relation to all data subjects is accurate. Data subjects must notify the data processor of any changes to information held about them. Data subjects have the right in some circumstances to request that inaccurate information about them is erased. This does not apply in all cases, for example, where records of mistakes or corrections are kept, or records which must be kept in the interests of all parties to which they apply.

Enforcement

If an individual believes that the business has not complied with this Policy or acted otherwise than in accordance with the Data Protection Act, the member of staff should utilise the business grievance procedure and should also notify the DPC.

Data Security

The business will take appropriate technical and organisational steps to ensure the security of personal data.

All staff will be made aware of this policy and their duties under the Act.

The business and therefore all staff and pupils are required to respect the personal data and privacy of others and must ensure that appropriate protection and security measures are taken against unlawful or unauthorised processing of personal data, and against the accidental loss of, or damage to all personal data.

An appropriate level of data security must be deployed for the type of data and the data processing being performed. In most cases, personal data must be stored in appropriate systems and be Data Protection Policy Lent 2017 4 encrypted when transported offsite. Other personal data may be for publication or limited publication within the business, therefore having a lower requirement for data security.

External Processors

The business must ensure that data processed by external processors, for example, service providers, Cloud services including storage, web sites etc. are compliant with this policy and the relevant legislation.

Secure Destruction

When data held in accordance with this policy is destroyed, it must be destroyed securely in accordance with best practice at the time of destruction.

Retention of Data

The business may retain data for differing periods of time for different purposes as required by statute or best practices, individual departments incorporate these retention times into the processes and manuals. Other statutory obligations, legal processes and enquiries may also necessitate the retention of certain data.

The business may store some data such as data capture, photographs, achievements, books and works etc. indefinitely in its archive.

Ethics and Anti-Bribery Policy

About Our Policy

It is the stated and publicly declared policy of the company to conduct all of our business in an honest and ethical manner.

The company will take a zero-tolerance approach to bribery and corruption. The company is committed to acting professionally, fairly and with integrity in all our business dealings and relationships.

Any employee who breaches this policy will face disciplinary action, which could result in dismissal for gross misconduct. Any non-employee who breaches this policy may have their contract terminated with immediate effect.

This policy does not form part of any employee's contract of employment and we reserve the right to amend or modify it at any time without prior notification.

As with all our policies the company will regularly review this policy to ensure it remains pertinent, relevant, and enforceable.

Within the Organisation – who must comply with this policy?

This policy applies to all persons working for Paternoster Communications Ltd or on our behalf in any capacity, including employees at all levels, directors, officers, agency workers, seconded workers, volunteers, interns, agents, contractors, external consultants, third-party representatives and business partners.

The definition of bribery?

Bribe means a financial or other inducement or reward for action which is illegal, unethical, a breach of trust or improper in any way.

Bribes can take the form of money, gifts, loans, fees, hospitality, services, discounts, the award of a contract or any other advantage or benefit.

– Bribery includes offering, promising, giving, accepting, or seeking a bribe.

– All forms of bribery are strictly prohibited.

– Specifically, our rules of engagement include

1. Employees must not give or offer any payment, gift, hospitality or other benefit in the expectation that a business advantage will be received in return, or to reward any business received
2. Employees may not accept any offer from a third party that is known or suspected to have been made with the expectation that a business advantage will be forthcoming
3. Employees may not give or offer any payment (sometimes called a facilitation payment) to a government official in any country to facilitate or speed up a routine or necessary procedure.

– Employees must not threaten or retaliate against another person who has refused to offer or accept a bribe or who has raised concerns about possible bribery or corruption.

Gifts and hospitality

– This policy does not prohibit the giving or accepting of reasonable and appropriate hospitality for legitimate purposes such as building relationships, maintaining our image or reputation, or marketing our products and services.

– A gift or hospitality will not be appropriate if it is unduly lavish or extravagant or could be seen as an inducement or reward for any preferential treatment (for example, during contractual negotiations or a tender process).

– Gifts must be of an appropriate type and value depending on the circumstances and taking account of the reason for the gift. Gifts must not include cash or cash equivalent (such as vouchers) or be given in secret. Gifts must be given in the name of the company and never in the name of an individual be they directly employed, associated with or connected to the company in any way.

– Promotional gifts of low value such as branded stationery may be given to or accepted from existing customers, suppliers, and business partners.

Record-keeping

– Employees must declare and keep a written record of all hospitality or gifts given or received. Employees must also submit all expenses claims relating to hospitality, gifts or payments to third parties in accordance with the company's expenses policy and record the reason for expenditure.

– All accounts, invoices, and other records relating to dealings with third parties including suppliers and customers should be prepared with strict accuracy and completeness. Accounts must not be kept "off-book" to facilitate or conceal improper payments.

How to raise a concern

If an employee or associate is offered a bribe, or are asked to make one, or if the employee and/or associate suspects any bribery, corruption or other breach of this policy has occurred or may occur, the Employee and/or the associate must notify the Founding Partner as to the possible breach, as soon as possible.