DATA PROTECTION POLICY

Introduction

Purpose

The organisation is committed to being transparent about how it collects and uses the personal data of its workforce, and to meeting its data protection obligations. This policy sets out the organisation's commitment to data protection, and individual rights and obligations in relation to personal data.

This policy applies to the personal data of job applicants, employees, workers, contractors, volunteers, interns, apprentices and former employees. It can also include customers, suppliers, business contacts, and other people the organisation has a relationship with or may need to contact.

The organisation has appointed Head of Governance as the person with responsibility for data protection compliance within the organisation

Data protection principles

The organisation processes personal data in accordance with the following data protection principles:

- The organisation processes personal data lawfully, fairly and in a transparent manner.
- The organisation collects personal data only for specified, explicit and legitimate purposes.
- The organisation processes personal data only where it is adequate, relevant and limited to what is necessary for the purposes of processing.
- The organisation keeps accurate personal data and takes all reasonable steps to ensure that inaccurate personal data is rectified or deleted without delay.
- The organisation keeps personal data only for the period necessary for processing.
- The organisation adopts appropriate measures to make sure that personal data is secure, and protected against unauthorised or unlawful processing, and accidental loss, destruction or damage.

The organisation tells individuals the reasons for processing their personal data, how it uses such data and the legal basis for processing in its privacy notices. It will not process personal data of individuals for other reasons. Where the organisation relies on its legitimate interests as the basis for processing data, it will ensure that this use will not override the rights and freedoms of individuals.

Where the organisation processes special categories of personal data or criminal records data to perform obligations or to exercise rights in employment law, this is done in accordance with a policy on special categories of data and criminal records data.

The organisation will update personal data promptly if an individual advises that his/her information has changed or is inaccurate.

The periods for which the organisation holds personal data are governed by statutory retention periods or as required for the business to carry out its duties.

The organisation keeps a record of its processing activities in respect of personal data in accordance with the requirements of the General Data Protection Regulation (GDPR).

Data security

The organisation takes the security of personal data seriously. The organisation has internal policies and controls in place to protect personal data against loss, accidental destruction, misuse or disclosure, and to ensure that data is not accessed, except by employees in the proper execution of their duties.

Where the organisation engages third parties to process personal data on its behalf, such parties do so on the basis of written instructions, are under a duty of confidentiality and are obliged to implement appropriate technical and organisational measures to ensure the security of data.

The organisation already has many technical and organizational measures in place,

- Server protection: Automated Patch Management, Antivirus and Malware Management, Vulnerability Management, Penetration Testing, Intrusion Detection & Prevention, Data Loss Prevention, Data Encryption, Identity & Access, Segregation of Duties and Privileged access
- Endpoint Protection: Automated Patch Management and Software deployment/rollback, AntiMalware,
- Network protection: Firewall Management, & Monitoring, Intrusion Detection & Prevention,
- Disaster Recovery & Business Continuity

Data breaches

If the organisation discovers that there has been a breach of personal data that poses a risk to the rights and freedoms of individuals, it will report it to the Information Commissioner within 72 hours of discovery. The organisation will record all data breaches regardless of their effect.

If the breach is likely to result in a high risk to the rights and freedoms of individuals, it will inform the affected individuals that there has been a breach and provide them with information about its likely consequences and the mitigation measures taken.

International data transfers

The organisation will not transfer personal data to countries outside the EEA.