DATA PROTECTION ACT STATEMENT AND POLICY

PURPOSE

The Data Protection Act ensures that anyone who has access to or uses others personal data, abides by the same set of principles.

The Data Protection Act exists in order to secure and respect an employee's right to privacy with regard to personal information that is held about him/her.

In giving new privacy rights to individuals, the Act puts responsibility on those who keep personal information. Anyone processing personal data must comply with the principles, as set out below.

PRINCIPLES

The principles of the Data Protection Act are that data will:

- ✓ Be obtained and processed fairly and lawfully.
- ✓ Be held only for specific and lawful purposes and must not be processed in a manner that is incompatible with those purposes.
- ✓ Be adequate, relevant, and not excessive for the purposes for which it is processed.
- ✓ Be accurate and where necessary kept up to date.
- ✓ Be held for no longer than is necessary for the purpose for which it is processed.
- ✓ Be processed in accordance with the rights of employees under the act.
- ✓ Be subject to appropriate security measures.
- ✓ Be subject to scrutiny by individuals who have the right to correct or erase inaccurate information.
- ✓ Not be transferred to countries outside the EEA without adequate protection.

SCOPE

The Data Protection Act and therefore this statement, covers employees, applicants, former applicants, agency workers, casual workers, and contract workers.

The Act regulates the processing of personal data that is either held on a computer or intended to be held on a computer or held in paper form in what the Act describes as a 'relevant filing system'.

The Personal Data Guardianship Code suggests five key principles of good data governance on which best practice is based. The organisation will seek to abide by this code in relation to all the personal data it processes, i.e.

- Accountability: those handling personal data follow publicised data principles to help gain public trust and safeguard personal data.
- Visibility: Data subjects should have access to the information about themselves that an organisation holds. This includes the right to have incorrect personal data corrected and to know who has had access to this data.
- Consent: The collection and use of personal data must be fair and lawful and in accordance with the DPA's eight data protection principles. Personal data should only be used for the purposes agreed by the data subject. If personal data is to be shared with a

third party or used for another purpose, the data subject's consent should be explicitly obtained.

- Access: Everyone should have the right to know the roles and groups of people within an organisation who have access to their personal data and who has used this data.
- Stewardship: Those collecting personal data have a duty of care to protect this data throughout the data life span

TYPE OF INFORMATION PROCESSED

- Forest Traffic Services processes the following personal information: Employees – background information covering Eligibility to Residential Address, Next of Kin, Work in the UK, Health information, Driving Licence, Bank and Tax Details.
- Personal information is kept in the following forms: Electronic (via secure server) and in hard copy (in secure fireproof storage cupboards)
- Groups of people within the organisation who will process personal information are: Human Resources, Finance, Safety and Management Board – are the only employee groups who will have access to personal information.

GATHERING AND CHECKING INFORMATION

- Before personal information is collected, we will consider the format that this data will be collected in and how it is stored and accessed in the future.
- We will inform people whose information is gathered about the following: The change in the way the information is handled and stored in the future.
- We will take the following measures to ensure that personal information kept is accurate: through occasional updates of personal information.
- Personal sensitive information will not be used apart from the exact purpose for which permission was given.

DATA SECURITY

The organisation will take steps to ensure that personal data is kept secure at all times against unauthorised or unlawful loss or disclosure. The following measures will be taken:

- Secure storage of hard data within lockable cupboards
- IT Systems with Security Log-on prompts
- Back-up data systems
- Files with sensitive data contain password-protection to prevent unauthorised or accidental access to such information.

Any unauthorised disclosure of personal data to a third party by an employee may result in disciplinary action.

SUBJECT ACCESS REQUESTS

Anyone whose personal information we process has the right to know:

- What information we hold and process on them
- How to gain access to this information
- How to keep it up to date
- What we are doing to comply with the Act.

They also have the right to prevent processing of their personal data in some circumstances and the right to correct, rectify, block or erase information regarded as wrong.
Individuals have a right under the Act to access certain personal data being kept about them on computer and certain files. Any person wishing to exercise this right should apply in writing to Tracey Evans, Financial Controller.
The following information will be required before access is granted: Proof of identification i.e., Valid Driving Licence or Passport
Queries about handling personal information will be dealt with swiftly and politely.
We will aim to comply with requests for access to personal information as soon as possible but will ensure it is provided within the 40 days required by the Act from receiving the written request.

REVIEW

This policy will be reviewed at intervals of 12 months to ensure it remains up to date and compliant with the law.

DEFINITIONS

Personal Data - data which relates to a living individual who can be identified from that data e.g., CV, performance development reviews, starter forms. This can be in manual or automatic records.

Processing Data - anything we do with data is, in effect, processing it including organisation, adaptation, alteration or retrieval.

Sensitive Data - information relating to racial or ethnic origin, political opinions, religious or other beliefs, trade union membership, health, sex life and criminal convictions. Legitimate reasons for processing such data may be for example, the monitoring of ethnic backgrounds and treatment of minorities, for the purposes of demonstrating and promoting equal opportunities policies.

Data Controller - determines how and for what purpose personal data is processed. Obligations in the Act fall mainly on data controllers. This is likely to be the Company rather than the workplace manager.

Failure to adhere to the principles of the Data Protection Act could result in disciplinary action.

Signed for and on behalf of Forest Traffic Services

Ross Williams
Managing Director
Forest Traffic Services
1st June 2021