**Privacy Notice**

**Introduction**

The Company is committed to protecting the privacy and security of your personal information. This privacy notice describes how we collect and use personal information about you during and after your working relationship with us, in accordance with the General Data Protection Regulation (GDPR) and Data Protection Act 2018 (DPA).

We are registered as a Data Controller with the Information Commissioner's Office (ICO). Our registration number is Z7546570.

This means that we are responsible for deciding how we hold and use personal information about you. We are required under data protection legislation to notify you of the information contained within this privacy notice.

This notice applies to current and former employees, agency workers, contractors, third party personnel and visitors to Magnox sites. It does not form part of any contract of employment or other contract to provide services. We may update this notice at any time.

It is important that you read this notice, together with any other privacy notice we may provide when we are collecting or processing personal information about you, so that you are aware of how and why we are using such information.

**Our Contact Details**

Data Protection Officer, Magnox Ltd

Oldbury Neate
Thornbury
South Gloucestershire
BS35 1RQ

Email: d.p.o@magnoxsites.com

**What type of information we have**

Personal data, or personal information, means any information about an individual from which that person can be identified. It does not include data where the identity has been removed (anonymised data). There are certain types of more sensitive personal data (special category data) which require a higher level of protection, such as information about a person's health or criminal convictions.

We may collect, store, and use the following categories of personal information about you:

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

• Date of birth;

• Gender;

• Marital status and dependants;

• Next of kin and emergency contact information;

• National Insurance number;

• Bank account details, payroll records and tax status information;

• Job title;

• Salary, annual leave, pension and benefits information;

• Start date and, if different, the date of your continuous employment;

• Leaving date and your reason for leaving;

• Location of employment or workplace;

• Copy of driving licence and car insurance;

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

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

• Compensation history;

• Performance information;

• Disciplinary and grievance information;

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

• CCTV images used to monitor access to buildings etc;

• Photographs;

• Passport details (including number, expiry date and place of issue);

• Computer username from Magnox Network (used as a unique identifier);

• Username, work number and title (for deployment of operating systems and software tools);

• Personal data related to the online training platform (including full name; corporate email address; module undertaken; completion status; assessment status; date undertaken & performance analytics).

Please note the above list is not exhaustive.

We may also collect, store and use the following more sensitive types of personal data:

• Information about your race or ethnicity, religious beliefs, sexual orientation and political opinions for equality and diversity monitoring purposes;

• Trade union membership;

• Information about your health, including any medical condition, health and sickness records etc;

• Details of any absences (other than holidays) from work including time on statutory parental leave and sick leave;

• Information about criminal convictions and offences;

• Biometric data, including fingerprint authorisation to access IT systems; and

• Dosimetry and radiological protection data

Please note the above list is not exhaustive.

**How did we get the information and why do we have it?**

We collect personal information about employees, agency workers, contactors & third party personnel through the application and recruitment process, either directly from candidates or sometimes from an employment agency. We may sometimes collect additional information from third parties including former employers, credit reference agencies or background check agencies. We also collect data from visitors to our sites for security and safety purposes, including name, date of birth, identity documentation, contact details and sometimes health data for access to certain facilities.

We will collect additional personal information in the course of job-related activities throughout the period that you work for us. We will only use your personal information when the law allows us to. Most commonly, we will use your personal information in the following circumstances, known as the ‘lawful basis for processing’:

• Contractual requirements;

• Compliance with a legal obligation;

• Provision of statutory functions or public task;

• Where it is necessary for legitimate interests pursued by us or a third party and your interests and fundamental rights do not override those interests. In accordance with best practice a Legitimate Interests Assessment (LIA) will be conducted when this lawful basis is used.

We may also use your personal information in the following situations, which are likely to be rare:

• To protect your interests (or someone else's interests);

• Where we have your consent.

Where we process special category data we need to identify both a lawful basis (as above) and a special category condition for processing in compliance with data protection legislation. The relevant conditions are likely to be:

• Employment;

• Occupational health;

• Explicit consent.

Please see the ‘Your data protection rights’ section for more information on withdrawing your consent.

**What we do with the information**

The situations in which we may process your personal information are listed below:

• Making a decision about your recruitment or appointment;

• Determining the terms on which you work for us;

• Checking you are legally entitled to work in the UK;

• Paying you and, if you are an employee or deemed employee for tax purposes, deducting tax and National Insurance contributions (NICs);

• Providing the following benefits to you:

- Annual leave entitlement

- Pension scheme

- Maternity and Paternity leave and pay

- Cycle to work scheme

- Car lease scheme

• Administering the contract we have entered into with you;

• Business management and planning, including accounting and auditing;

• Conducting performance reviews, managing performance and determining performance requirements;

• Making decisions about salary reviews and compensation;

• Assessing qualifications for a particular job or task, including decisions about promotions;

• Gathering evidence for possible grievance or disciplinary hearings;

• Making decisions about your continued employment or engagement;

• Making arrangements for the termination of our working relationship;

• Education, training and development requirements;

• Dealing with legal disputes involving you, or other employees, workers and contractors, including accidents at work;

• Ascertaining your fitness to work;

• Managing sickness absence;

• Complying with health and safety obligations;

• To prevent fraud;

• To make travel arrangements, via a third party data processor, with organisations who provide travel services;

• To monitor your use of our information and communication systems to ensure compliance with our IT policies;

• To ensure network and information security, including preventing unauthorised access to our computer and electronic communications systems and preventing malicious software distribution;

• To conduct data analytics studies to review and better understand employee retention and attrition rates;

• Equal opportunities monitoring;

• To create records in, and allow access to, the cloud based learning management system (LMS);

• To protect staff from the health risks of working with display screen equipment (DSE), such as PCs, laptops, tablets and smartphones;

• Complying with legal, statutory and regulatory obligations including reporting to government on salaries of higher earners;

• To identify potential locations for hub offices we would like to identify possible sites for hub offices which would support our employees working in a more flexible way. To determine which locations might be appropriate for consideration, it is necessary for us to understand the ‘heat map’ of areas where our employees currently live, compared to our existing offices.

• Allowing access to Magnox sites for visitors; checking of identity & clearance information for security purposes, to allow access to secure areas where protectively marked/nuclear sensitive material may being handled.

Some of the above grounds for processing will overlap and there may be several grounds which justify our use of your personal information.

If you wish to know more about which legal basis Magnox uses to process your personal data then please contact the Data Protection Officer

If you fail to provide certain information when requested, we may not be able to perform the contract we have entered into with you (such as paying you or providing a benefit), or we may be prevented from complying with our legal obligations (such as to ensure the health and safety of our workers).

**Change of purpose**

We will only use your personal information 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. If we need to use your personal information for an unrelated purpose, we will notify you and we will explain the legal basis which allows us to do so.

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

**Do we need your consent?**

We do not need your consent if we use special category personal data in accordance with our written policy to carry out our legal obligations or exercise specific rights in the field of employment law. In limited circumstances, we may approach you for your written consent to allow us to process certain particularly sensitive data. If we do so, we will provide you with full details of the information that we require and the reason we need it, so that you can carefully consider whether you wish to consent. You should be aware that it is not a condition of your contract with us that you agree to any request for consent from us.

**Information about criminal convictions**

We will only collect information about criminal convictions if it is appropriate given the nature of the role and where we are legally able to do so. The information will be collected as part of the recruitment process or we may be notified directly by yourself in the course of you working for us.

All processing will be in line with our data protection policy and adhere to prevailing data protection legislation.

**Automated decision-making**

Automated decision-making takes place when an electronic system uses personal information to make a decision without human intervention. We do not envisage that any decisions will be taken about you using automated means, however we will notify you in writing if this position changes.

**How we store your information**

We have put in place appropriate security measures to prevent your personal information from being accidentally lost, used or accessed in an unauthorised way, altered or disclosed. In addition, we limit access to your personal information to those employees, agents, contractors and other third parties who have a business need to know. They will only process your personal information on our instructions and they are subject to a duty of confidentiality. Details of these measures may be obtained from the Data Protection Officer.

The following activities are carried out by third-party service providers:

• Regulators (e.g. HMRC, HSE)

• Pension administration;

• Benefits provision;

• Online platform to deliver and manage training modules to ensure staff can perform their job within the expected organisational requirements. This online platform is managed by a third party provider that hosts the Learning Management System (LMS), this is a cloud based service using the SaaS service model;

• Occupational health;

• Trade union membership;

• Travel arrangements (air, rail etc.);

• Dosimetry and epidemiological services

We have put in place procedures to deal with any suspected data security breach and will notify you and any applicable regulator of a suspected breach where we are legally required to do so.

We may also transfer your personal data outside of the EU. If this is the case you can expect a similar degree of protection in respect of your personal information.

We will only hold onto your personal information for as long as necessary to fulfil the purposes we collected it for. All records are retained and securely destroyed in accordance with our records retention schedule. Details of retention periods for different aspects of your personal data are available upon request. However, your information may be held beyond the specified retention periods where there is the potential for it to be required for legal purposes.

**Your data protection rights**

Data protection legislation strengthens the rights of individuals and includes:

• The right to be informed (which this notice fulfils);

• The right of access;

• The right to rectification;

• The right to erasure;

• The right to restrict processing;

• The right to data portability;

• The right to object;

• Rights in relation to automated decision making and profiling.

For a detailed explanation of these rights, and the specific circumstances in which they apply, please visit the Information Commissioners Office (ICO) website.

If you wish to exercise any of your rights, including where you are seeking a copy of your own personal information, please contact the DPO via d.p.o@magnoxsites.com.

**How to complain**

If you wish to make a complaint to Magnox Limited about the way in which we have processed your personal information please contact the DPO using the email address above.

If you remain dissatisfied with the response received, you have the right to lodge a complaint to the ICO. The ICO is the UK's independent body set up to uphold information rights, and they can investigate and adjudicate on any data protection related concerns you raise with them. They can be contacted at:

Information Commissioner’s Office

Wycliffe House, Water Lane,

Wilmslow,

Cheshire,

SK9 5AF

0303 123 1113

ico.org.uk