UKEL is committed to protecting your personal data and respecting your privacy. Our Data Protection Policy explains how we collect, use, store and protect information about visitors to our website and individuals who interact with us.

We make every effort to guarantee the accuracy of information contained within this site, but we accept no liability for any inaccuracies and visitors who rely on this information do so at their own risk.

UKEL is not responsible for the contents or reliability of websites we link to and links shall not be taken as an endorsement.

Please contact us at hello@ukel.co.uk if you have any questions on our policy or website content.

UKEL

DATA PROTECTION POLICY

1. Introduction and scope

1.1. Everyone has rights about the way in which their personal data is handled. Personal Data is any information identifying an individual or information relating to a living, identified or identifiable individual (Data Subject) that we can identify – directly or indirectly - from that data alone or in combination with other identifiers we possess or can reasonably access. During the course of our activities we will collect, store and process Personal Data about our stakeholder, suppliers, event participants, employees, volunteers and other third parties, and we recognise that the correct and lawful treatment of this data will maintain confidence in the organisation and will provide for successful business operations.

1.2. UKEL is committed to a policy of protecting the rights and privacy of individuals in accordance with the Data Protection Laws. The retained EU law version of the General Data Protection Regulation (UK GDPR) and the Data Protection Act 2018 demand high transparency and accountability in how UKEL manages and uses Personal Data. It also accords rights for individuals to understand and control that use.

1.3. Data Users are obliged to comply with this policy when processing personal data on our behalf. Any breach of this policy may result in disciplinary action.

1.4. The Data Protection Laws all require that the personal data is processed in accordance with the Data Protection Principles (on which see below) and gives individuals rights to access, correct and control how we use their personal data (on which see below).

1.5. The types of personal data that UKEL may be required to handle include information about current, past and prospective suppliers, customers, clients, students and others that we communicate with. The personal data, which may be held on paper or on a computer or other media, is subject to certain legal safeguards specified in the Data Protection Laws.

1.6. This policy and any other documents referred to in it sets out the basis on which we will process any personal data we collect from data subjects, or that is provided to us by data subjects or other sources.

1.7. This policy does not form part of any employee's contract of employment we reserve the right to amend this policy at any time. Where appropriate, we will notify employees and key volunteers of those changes by mail or email.

1.8. This policy sets out rules on data protection and the legal conditions that must be satisfied when we obtain, handle, process, transfer and store personal data. This policy should be read in conjunction with the Data Breach Policy, the Data Retention Policy, and the applicable Privacy Notices.

1.9. The Data Protection Officer (DPO) is responsible for ensuring compliance with the Data Protection Laws and with this policy. This post is held by Bev Ward, COO, (bevward@ukel.co.uk). Any questions about the operation of this policy or any concerns that the policy has not been followed should be referred in the first instance to the DPO.

1.10. The Data Protection Laws are not intended to prevent the processing of personal data, but to ensure that it is done fairly and without adversely affecting the rights of the data subject.

1.11. For personal data to be processed lawfully, they must be processed on the basis of one of the legal grounds set out in the Privacy Notices. These include, among other things, the data subject's consent to the processing, or that the processing is necessary for the performance of a contract with the data subject, for the compliance with a legal obligation to which the data controller is subject, or for the legitimate interest of the data controller or the party to whom the data is disclosed. When Special Categories of data is being processed, additional conditions must be met. When processing personal data as data controllers in the course of our business, we will ensure that those requirements are met

2. Definition of Data Protection Terms

2.1. Data is information which is stored electronically, on a computer, or in certain paper-based filing systems.

2.2. Data subjects for the purpose of this policy include all living individuals about whom we hold personal data including for our employees. A data subject need not be a UK national or resident. All data subjects have legal rights in relation to their personal information.

2.3. Personal data means data relating to a living individual who can be identified from that data (or from that data and other information in our possession). Personal data can be factual (for example, a name, address, email address or date of birth) or it can be an opinion about that person, their actions and behaviour.

2.4. Data controllers are the people who, or organisations which, determine the purposes for which, and the manner in which, any personal data is processed. They are responsible for establishing practices and policies in line with the Data Protection Laws. We are the data controller of all personal data used in our business for our own purposes.

2.5. Data users are those of our employees and key volunteers whose work involves processing personal data. Data users must protect the data they handle in accordance with this data protection policy and any applicable data security procedures at all times.

2.6. Data processors include any person or organisation that is not a data user that processes personal data on our behalf and on our instructions. Employees of data controllers are excluded from this definition but it could include suppliers which handle personal data on UKEL's behalf.

2.7. Processing is any activity that involves use of the 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 transferring personal data to third parties.

2.8. We may also collect, store and use the "special categories" of more sensitive personal information Special categories includes information about a person's racial or ethnic origin, political opinions, religious or similar beliefs, trade union membership, physical or mental health or condition or sexual life, or about the commission of, or proceedings for, any offence committed or alleged to have been committed by that person, the disposal of such proceedings or the sentence of any court in such proceedings. Special categories of personal data can only be processed under strict conditions, including a condition requiring the express permission of the person concerned.

3. Data Protection Principles

3.1. Anyone processing personal data must comply with the eight enforceable principles of good practice. These provide that personal data must be:

a) Processed fairly and lawfully.
b) Processed for limited purposes and in an appropriate way.
c) Adequate, relevant and not excessive for the purpose.
d) Accurate.
e) Not kept longer than necessary for the purpose.
f) Processed in line with data subjects' rights.
g) Secure.
h) Not transferred to people or organisations situated in countries outside the EEA without adequate protection.

4. Lawfulness, Fairness and Transparency

4.1. Personal data must be Processed lawfully, fairly and in a transparent manner in relation to the Data Subject.

4.2. The Data Protection Laws specify that data controllers may only collect, process and share Personal Data fairly and lawfully and for specified purposes.

4.3. The UK GDPR restricts our actions regarding Personal Data to specified lawful purposes. The UK GDPR allows Processing for specific purposes, some of which are set out below:

a) the Data Subject has given their Consent;
b) the Processing is necessary for the performance of a contract with the Data Subject;
c) to meet our legal compliance obligations;
d) to protect the Data Subject's vital interests;

e) to pursue our legitimate interests (or those of a third party) for purposes where they are not overridden because the Processing prejudices the interests or fundamental rights and freedoms of Data Subjects.

4.4. Further information on the purposes for which we process different categories of Personal Data are set out in our Privacy Notices.

5. Data Protection Rights

5.1. In the course of our business, we may collect and process the personal data set out in the Privacy Notices. This may include data we receive directly from a data subject (for example, by completing forms or by corresponding with us by mail, phone, email or otherwise) and data we receive from other sources (including, for example, business partners, sub-contractors in technical, payment and delivery services, credit reference agencies and others).

5.2. We will only process personal data for the specific purposes set out in the Privacy Notices or for any other purposes specifically permitted by the Data Protection Laws. We will notify those purposes within the Privacy Notice to the data subject when we first collect the data or as soon as possible thereafter.

5.3. Under data protection laws individuals have certain rights in relation to their own personal data. In summary these are:

a) The rights to access their personal data, usually referred to as a subject access request; The right to have their personal data rectified;
b) The right to have their personal data erased, usually referred to as the right to be forgotten;
c) The right to restrict processing of their personal data;
d) The right to object to receiving direct marketing materials;
e) The right to portability of their personal data;
f) The right to object to processing of their personal data; and
g) The right to not be subject to a decision made solely by automated data processing.

5.4. Not all of these rights are absolute rights, some are qualified and some only apply in specific circumstances.

5.5. Anyone wishing to exercise any of these rights should apply in writing to the DPO. Any member of UKEL staff receiving any such request shall forward it to the DPO.

5.6. When receiving telephone enquiries, we will only disclose personal data we hold on our systems if the following conditions are met:

a) We will check the caller's identity to make sure that information is only given to a person who is entitled to it.
b) We will suggest that the caller put their request in writing if we are not sure about the caller's identity and/or where their identity cannot be checked.

c) UKEL personnel will refer requests to a more senior UKEL representative, and/or the DPO, for assistance in difficult situations. UKEL will not tolerate any harassment or intimidation of its employees who are carrying out their duties in accordance with this policy.

6. Security

6.1. UKEL has an obligation to put in place appropriate technical and organisational measures to protect against unauthorised or unlawful processing of personal data, and against accidental loss or destruction of data.

6.2. We will ensure that all personal data is accessible only to those who have a valid reason for using it. We will have in place appropriate security measures such as password protecting personal data held electronically and ensuring personal data is accessible only to those who have a valid reason for using it.

6.3. The organisation backs up data every day. Backups are kept in the cloud and are verified regularly by the software and system supplier.

6.4. Master copies of software are stored in cloud storage that is backed up to another cloud storage.

6.5. All end user devices, servers and network equipment are configured to install security patches and firmware updates within 14 days of them being released by the vendor.

6.6. Firewall and Malware protection are automatically updated with high priority updates and Staff are given annual security awareness training to ensure they are equipped to respond to the latest security threats.

6.7. The organisation plans for how to deal with loss of electricity, external data links, server failure and network problems.

UKEL – DATA PROTECTION POLICY	
Approved	October 2025
Review Scheduled	October 2026