Data Protection Handbook

Issue Date:	22nd May, 2018
Revision Number:	Issue 1

Table of Contents

Employee Data Protection Policy

Keltech Engineering is committed to protecting the privacy and security of your personal information. We are a data controller. This means we are responsible for deciding how we hold and use personal information about you. This notice explains to you what decisions we have taken in relation to that information.

Introduction:

This policy 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). We encourage you to read this policy carefully, together with any other privacy notice we may provide on specific occasions when we are collecting or processing personal information about you, so that you are aware of how and why we are using such information. It applies to all employees.

We have appointed a Data Protection Officer (DPO) to oversee compliance with this policy. If you have any questions about this policy or how we handle your personal information, please contact the Martin Freyne, IT Officer. As a data controller, we are responsible for deciding how we hold and use personal information about you. This policy explains to you what decisions we have taken in relation to that information.

General Data Protection Principles:

In collecting and processing your personal information, we will comply with the data protection law in force at the time. This requires that the personal information we hold about you must be:

- Used lawfully, fairly and in a transparent way.
- Collected only for valid purposes that we have clearly explained to you and not used in any way that is incompatible with those purposes.
- Relevant to the purposes we have told you about and limited only to those purposes.
- Accurate and kept up to date.
- Kept only as long as necessary for the purposes we have told you about.
- Kept securely.

Legal Basis for Processing:

In order to collect and process personal data “lawfully”, Keltech must have a legal basis for doing so. There are six available legal bases for processing. No single basis is ‘better’ or more important than the others – which basis is most appropriate to use will depend on the purpose and the relationship with the individual. The six legal bases, set out in Article 6(1) of the GDPR, are as follows:

- Consent**:** The individual has given clear consent for Keltech to process their personal data for a specific purpose.

- Contract**:** The processing is necessary for a contract Keltech has with the individual, or because they have asked Keltech to take specific steps before entering into a contract.
- Legal obligation**:** The processing is necessary for Keltech to comply with the law.
- Vital interests: the processing is necessary to protect someone's life.
- Public task: The processing is necessary for Keltech to perform a task in the public interest or for its official functions.
- Legitimate interests**:** The processing is necessary for the legitimate interests of the Keltech or a third party.

The kind of information we hold about you:

We will collect, store, and use a variety of categories of personal information about you. Those categories are detailed in the Schedule to this policy. We may also collect, store and use "special categories" of more sensitive personal information, which are also detailed in the Schedule to this policy.

How is your personal information collected:

We collect personal information about our employees 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. We will collect additional personal information in the course of job-related activities throughout the period of you working for us.

How we will use information about you:

We will only use your personal information when the law allows us to and as detailed in the Schedule to this policy.

If you fail to provide personal information:

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 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 to use particularly sensitive information?

We do not need your consent if we use your personal information 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 would like 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.

Why might you share my personal information with third parties?

We may have to share your data with third parties, including third-party service providers. We require third parties to respect the security of your data and to treat it in accordance with the law. However, we will only share your personal information with third parties where required by law.

Data security:

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 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 DPO. 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.

Data retention:

We will only retain your personal information for as long as necessary to fulfil the purposes we collected it for, including for the purposes of satisfying any legal, accounting, or reporting requirements. Details of retention periods for different aspects of your personal information are set out in the Schedule to this policy. In some circumstances we may anonymise your personal information so that it can no longer be associated with you, in which case we may use such information without further notice to you.

Your duty to inform us of changes:

It is important that the personal information we hold about you is accurate and current. Please keep us informed if your personal information changes during your working relationship with us.

Your rights in connection with personal information:

Under certain circumstances, the law grants you specific rights. These are summarised below. Please note that your rights may be limited and subject to restrictions in certain situations:

Request access to your personal information (commonly known as a “data subject access request”). This enables you to receive a copy of the personal information we hold about you and to check that we are lawfully processing it.

- Request correction of the personal information that we hold about you. This enables you to have any incomplete or inaccurate information we hold about you corrected.

- Request erasure of your personal information. This enables you to ask us to delete or remove personal information where there is no good reason for us continuing to process it. You also have the right to ask us to delete or remove your personal information where you have exercised your right to object to processing (see below).
- Object to processing of your personal information where we are relying on a legitimate interest (or those of a third party) and there is something about your particular situation which makes you want to object to processing on this ground. You also have the right to object where we are processing your personal information for direct marketing purposes.
- Request the restriction of processing of your personal information. This enables you to ask us to suspend the processing of personal information about you, for example if you want us to establish its accuracy or the reason for processing it.
- Request the transfer of your personal information to another party.

If you want to review, verify, correct or request erasure of your personal information, object to the processing of your personal data, or request that we transfer a copy of your personal information to another party, please contact the DPO.

You will not have to pay a fee to access your personal information (or to exercise any of the other rights). However, we may charge a reasonable fee if your request for access is unfounded or excessive. Alternatively, we may refuse to comply with the request in such circumstances.

Schedule:

In this schedule Keltech has established retention or destruction schedules for specific categories of records, this is done to ensure legal compliance.

Personnel Records		
Record	Retention Period	Basis
Employee applications and resumes	1 Year and 1 Day or where successful, for the duration of the employment plus 3 years from date of termination of employment.	Legal Basis to Execute Contract
Employee offer letters (and other documentation regarding hiring, promotion, demotion, transfer, termination or selection for training)	1 Year and 1 Day or where successful, for the duration of the employment plus 3 years from date of termination of employment.	Legal Basis to Execute Contract and facilitate returning employees and employees seeking training records for new employer (training certificates generally last 3 years).
Records relating to background checks on employees	1 Year and 1 Day or where successful, for the duration of the employment plus 3 years from date of termination of employment.	Legal Basis to Execute Contract

Employment contracts; employment and termination agreements	Duration of the employment plus 3 years from end of calendar year from date of termination of employment.	Legal Basis to Execute Contract
Injury and Illness Incident Reports and related Annual Summaries; Logs of work-related injuries and illnesses	Duration of the employment plus 3 years from end of calendar year from date of termination of employment.	Legal Basis to Execute Contract and Vital Interest to ensure employee safety and wellbeing.
Job descriptions, performance goals and reviews;	Duration of the employment plus 3 years from end of calendar year from date of termination of employment.	Legal Basis to Execute Contract
Written allegations/ complaints	Duration of the employment plus 3 years from end of calendar year from date of termination of employment.	Legal Basis to Execute Contract and Vital Interest to ensure employee safety and wellbeing.
Log and Summary of Occupational Injuries and Illnesses	Duration of the employment plus 3 years from end of calendar year from date of termination of employment.	Legal Basis to Execute Contract and Vital Interest to ensure employee safety and wellbeing.
Injury and Illness Incident Reports and related Annual Summaries; Logs of work-related injuries and illnesses	Duration of the employment plus 3 years from end of calendar year from date of termination of employment.	Legal Basis to Execute Contract and Vital Interest to ensure employee safety and wellbeing.

Payroll Records		
Record	Retention Period	Basis
Employee records with information on pay rate or weekly compensation	7 Years from end of calendar year.	Legal Basis to Execute Contract
Employee tax records	7 Years from end of calendar year.	Legal Basis to Execute Contract
Time reports	7 Years from end of calendar year.	Legal Basis to Execute Contract
Superannuation / Pension/ Retirement records	7 Years from end of calendar year.	Legal Basis to Execute Contract
Payroll registers (gross and net)	7 Years from end of calendar year.	Legal Basis to Execute Contract
Clock in times; wage rate tables; pay rates; work and time	7 Years from end of calendar year.	Legal Basis to Execute Contract

schedules; earnings records; records of additions to or deductions from wages; records on which wage computations are based		

Data Protection Introduction

Purpose of this Document

The Data Protection Acts 1988 and 2003 (as amended) (the **DPA**) and, from the 25th of May 2018, the General Data Protection Regulation (the **GDPR**) impose obligations on us, as a Data Controller, to process personal data in a fair manner which notifies data subjects of the purposes of data processing and to retain the data for no longer than is necessary to achieve those purposes.

Under these rules, individuals have a right to be informed about how their personal data is processed. The GDPR sets out the information that we should supply to individuals and when individuals should be informed of this information. We are obliged to provide individuals with information on our retention periods or criteria used to determine the retention periods.

Grounds for Processing

Under the DPAs and the GDPR, Keltech are required to provide data subjects with the legal grounds or lawful basis that they are relying on for processing personal data.

The legal grounds for processing personal data are as follows:

- Consent;
- Performance of a contract;
- Legal obligation;
- Vital interest;
- Public interest; or Legitimate interests.

Explicit consent is required where special categories, also known as sensitive personal data are being processed.

Keltech may be able to rely a number of legal bases for collecting personal data. For example, as employers, Keltech can justify processing an employee's personal data as necessary for the performance of a contract and as part of a statutory requirement.

If there is no justification for retaining personal information, then that information should be routinely deleted. Information should never be kept "just in case" a use can be found for it in the future. If we want to retain information about our employees or clients to help us to provide a better service to them in the future, we must obtain their consent in advance.

Further Processing

Further retention of the personal data should be lawful only when it is compatible with the purposes for which it was originally collected. In this case no separate legal basis is

required - it should be relied on where it is necessary, for exercising the right of freedom of expression and information, for compliance with a legal obligation, for the performance of a task carried out in the public interest or in the exercise of official authority vested in the data controller, on the grounds of public interest in the area of public health, for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes, or for the establishment, exercise or defence of legal claims.

Right of Erasure

Individuals have the right to have their personal data erased and no longer processed in the following circumstances:

- Where the personal data are no longer necessary in relation to the purposes for which they are collected or otherwise processed, or
- Where a data subject has withdrawn his or her consent or objects to the processing of personal data concerning him or her,
- Where the processing of his or her personal data does not otherwise comply with the GDPR.

That right is relevant in particular where the data subject has given his or her consent as a child and is not fully aware of the risks involved by the processing, and later wants to remove such personal data, especially on the internet.

The data subject should be able to exercise that right notwithstanding the fact that he or she is no longer a child

Legal Basis for Processing

In order to collect and process personal data “lawfully”, Keltech must have a legal basis for doing so. There are six available legal bases for processing. No single basis is ‘better’ or more important than the others – which basis is most appropriate to use will depend on the purpose and the relationship with the individual. The six legal bases, set out in Article 6(1) of the GDPR, are as follows:

- **Consent**: the individual has given clear consent for the University to process their personal data for a specific purpose.
- **Contract**: the processing is necessary for a contract the University has with the individual, or because they have asked the University to take specific steps before entering into a contract.
- **Legal obligation**: the processing is necessary for the University to comply with the law.
- **Vital interests:** the processing is necessary to protect someone’s life.
- **Public task:** the processing is necessary for the University to perform a task in the public interest or for its official functions.
- **Legitimate interests**: the processing is necessary for the legitimate interests of the University or a third party.

GDPR Definitions

For the avoidance of doubt, and for consistency in terminology, the following definitions will apply within this Policy.

Data	This includes both automated and manual data. Automated data means data held on computer or stored with the intention that it is processed on computer. Manual data means data that is processed as part of a relevant filing system, or which is stored with the intention that it forms part of a relevant filing system.
Personal Data	Information which relates to a living individual, who can be identified either directly from that data, or indirectly in conjunction with other data which is likely to come into the legitimate possession of the Data Controller.
Sensitive Personal Data	A particular category of Personal data, relating to: Racial or Ethnic Origin, Political Opinions, Religious, Ideological or Philosophical beliefs, Trade Union membership, Information relating to mental or physical health, information in relation to one's Sexual Orientation, information in relation to commission of a crime and information relating to conviction for a criminal offence.
Data Controller	A person or entity who, either alone or with others, controls the content and use of Personal Data by determining the purposes and means by which that Personal Data is processed.
Data Subject	A living individual who is the subject of the Personal Data, i.e. to whom the data relates either directly or indirectly.
Data Processor	A person or entity who processes Personal Data on behalf of a Data Controller on the basis of a formal, written contract, but who is not an employee of the Data Controller, processing such Data in the course of his/her employment.
Data Protection Officer	A person appointed by Keltech to monitor compliance with the appropriate Data Protection legislation, to deal with Subject Access Requests, and to respond to Data Protection queries from staff members and service recipients.
Relevant Filing System	Any set of information in relation to living individuals which is not processed by means of equipment operating automatically (computers), and that is structured, either by reference to individuals, or by reference to criteria relating to individuals, in such a manner that specific information relating to an individual is readily retrievable.

Data Retention Procedure

Introduction

As a company, we are required to retain certain records, usually for a specific amount of time. The accidental or intentional destruction of these records during their specified retention periods could result in the following consequences:

- Fines and penalties.
- Loss of rights.
- Obstruction of justice charges.
- Contempt of court charges.
- Serious disadvantages in litigation.

We must retain certain records because they contain information that:

- Serves as Keltech's' corporate memory.
- Have enduring business value (for example, they provide a record of a business transaction, protect our legal interests or ensure operational continuity.
- Must be kept in order to satisfy legal, accounting or other regulatory requirements.

We must balance these requirements with our statutory obligation to only keep records for the period required and to comply with data minimisation principles. The retention schedule below sets out the relevant periods for the retention of Keltech's documents.

Types of Documents

This section explains the differences among records, disposable information, personal data and confidential information belonging to others.

Records

A record is any type of information created, received or transmitted in the transaction of Keltech's business, regardless of physical format. Examples of where the various types of information are located are:

- Audio and video recordings.
- Computer programs.
- Contracts.
- Electronic files.
- E-mails.
- Handwritten notes.
- Invoices.
- Letters and other correspondence.
- Magnetic tape.
- Memory in mobile phones and PDAs.
- Online postings, such as on Facebook, Twitter, Linkedin and other sites.
- Performance reviews.

Therefore, any paper records and electronic files, that are part of any of the categories listed in the Records Retention Schedule contained in the Appendix to this policy, must be retained for the amount of time indicated in the Records Retention Schedule.

A record must not be retained beyond the period indicated in the Record Retention Schedule, unless a valid business reason (or a litigation hold or other special situation) calls for its continued retention.

If you are unsure whether to retain a certain record, contact the Data Protection Officer.

Our Data Protection Officer is: Martin Freyne: Martin.Freyne@keltech.ie

Disposable Information

Disposable information consists of data that may be discarded or deleted at the discretion of the user once it has served its temporary useful purpose and/or data that may be safely destroyed because it is not a record as defined by this policy. Examples may include:

- Duplicates of originals that have not been annotated.
- Preliminary drafts of letters, memoranda, reports, worksheets and informal notes that do not represent significant steps or decisions in the preparation of an official record.
- Books, periodicals, manuals, training binders and other printed materials obtained from sources outside of Securitas and retained primarily for reference purposes.
- Spam and junk mail.

Personal Data

Personal Data is defined as any data which can identify an individual either on its own or when combined with other data which we possess. Some examples of personal data include names and addresses, email addresses, CVs, details of previous employment, medical records and references.

Confidential Information Belonging to Others

Any confidential information that an employee may have obtained from a source outside of Keltech, such as a previous employer, must not, so long as such information remains confidential, be disclosed to or used by Keltech. Unsolicited confidential information submitted to Keltech should be refused, returned to the sender where possible and deleted, if received via the internet.

Data Protection Officer in Records Management

Our Data Protection Officer, in conjunction with senior management, is responsible for identifying the documents that Keltech must or should retain, and determining, in collaboration with the Finance and HR Departments, the proper period of retention.

The responsibilities of the Data Protection Officer include:

- Arranging for the proper storage and retrieval of records, coordinating with outside vendors where appropriate.
- Handling the destruction of records whose retention period has expired.
- Planning, developing and prescribing document disposal policies, systems, standards and procedures.
- Monitoring departmental compliance so that employees know how to follow the document management procedures and the company has confidence that Securitas' records are controlled.
- Ensuring that senior management is aware of their departments' document management responsibilities.
- Developing and implementing measures to ensure that the company knows what information Keltech has and where it is stored, that only authorised users have access to the information, and that Keltech keeps only the information it needs, thereby efficiently using space.
- Establishing standards for filing and storage equipment and recordkeeping supplies.
- In cooperation with department heads, identifying essential records and establishing a disaster plan for each office and department to ensure maximum availability of Keltech's records in order to re-establish operations quickly and with minimal interruption and expense.
- Periodically reviewing the records retention schedules and legislation to determine if Keltech's document management program and its Records Retention Schedule is in compliance with legislation.
- Informing the various department heads of any laws and administrative rules relating to corporate records.
- In conjunction with the HR Department explaining to employees their duties relating to the document management program.
- Ensuring that the maintenance, preservation, computer disk storage, destruction or other disposition of Keltech's records is carried out in accordance with this policy, the procedures of the document management program and our legal requirements.
- Planning the timetable for the annual records destruction exercise and the annual records audit, including setting deadlines for responses from departmental staff.
- Evaluating the overall effectiveness of the document management program.
- Reporting regularly to the Senior Management on GDPR related issues within the company.

Store and Destruction of Records

Storage

Keltech's records must be stored in a safe, secure and accessible manner. Any documents and financial files that are essential to our business operations during an emergency must be duplicated and/or backed up at least once per week and maintained off site.

Destruction

Keltech is responsible for the continuing process of identifying the records that have met their required retention period and supervising their destruction. The destruction of personal data, confidential, financial and personnel-related records must be conducted by shredding for hard copy and standard deletion for soft copy files.

Data Requests Procedure

Purpose:

This procedure sets out the key features regarding handling or responding to requests for access to personal data made by data subjects, their representatives or other interested parties. This procedure will enable us to comply with legal obligations, provide better customer care, improve transparency, enable individuals to verify that information held about them is accurate, and increase the level of trust by being open with individuals about the information that is held about them. This procedure applies to employees that handle data subject access requests such as the Data Protection Officer.

Data Subject Access Request ("DSAR")

A Data Subject Access Request (DSAR) is any request made by an individual or an individual's legal representative for information held by the Company about that individual. The Data Subject Access Request provides the right for data subjects to see or view their own personal data as well as to request copies of the data. A Data Subject Access Request must be made in writing.

In general, verbal requests for information held about an individual are not valid DSARs. In the event a formal Data Subject Access Request is made verbally to a staff member of the Company, further guidance should be sought from Data Protection Officer, who will consider and approve all Data Subject Access Request applications.

The Rights of a Data Subject

The rights to data subject access include the following:

- Know whether a data controller holds any personal data about them.
- Receive a description of the data held about them and, if permissible and practical, a copy of the data.
- Be informed of the purpose(s) for which that data is being processed, and from where it was received.
- Be informed whether the information is being disclosed to anyone apart from the original recipient of the data; and if so, the identity of those recipients.
- The right of data portability. Data subjects can ask that their personal data be transferred to them or a third party in machine readable format (Word, PDF, etc.).

However, such requests can only be fulfilled if the data in question is:

1) provided by the data subject to the Company,

2) is processed automatically and

3) is processed based on consent or fulfilment of a contract.

- If the data is being used to make automated decisions about the data subject, to be told what logic the system uses to make those decisions and to be able to request human intervention.

The Company must provide a response to data subjects requesting access to their data within 30 calendar days of receiving the Data Subject Access Request unless local legislation dictates otherwise.

Requirements for a valid DSAR

In order to be able to respond to the Data Subject Access Requests in a timely manner, the data subject should:

- Submit his/her request using a Data Subject Access Request Form.
- Provide the Company with sufficient information to validate his/her identity (to ensure that the person requesting the information is the data subject or his/her authorized person).

Subject to the exemptions referred to in this document, the Company will provide information to data subjects whose requests are in writing (or by some other method explicitly permitted by the local law), and are received from an individual whose identity can be validated by company.

However, the company will not provide data where the resources required to identify and retrieve it would be excessively difficult or time-consuming. Requests are more likely to be successful where they are specific and targeted at particular information.

Factors that can assist in narrowing the scope of a search include identifying the likely holder of the information (e.g. by making reference to a specific department), the time period in which the information was generated or processed (the narrower the time frame, the more likely a request is to succeed) and being specific about the nature of the data sought (e.g. a copy of a particular form or email records from within a particular department).

DSAR Process

Request

Upon receipt of a DSAR, the Data Protection Officer will acknowledge the request. The requestor may be asked to complete a Data Subject Access Request Form to better enable the Company to locate the relevant information.

Identity verification

The Data Protection Officer needs to check the identity of anyone making a DSAR to ensure information is only given to the person who is entitled to it. If the identity of a DSAR requestor has not already been provided, the person receiving the request will ask the requestor to provide two forms of identification, one of which must be a photo identity and the other confirmation of address. If the requestor is not the data subject, written confirmation that the requestor is authorized to act on behalf of the data subject is required.

Information for Data Subject Access Request

Upon receipt of the required documents, the person receiving the request will provide the Data Protection Officer with all relevant information in support of the DSAR. Where the Data Protection Officer is reasonably satisfied with the information presented by the person who received the request, the Data Protection Officer will notify the requestor that his/her DSAR will be responded to within 30 calendar days. The 30 day period begins from the date that the required documents are received. The requestor will be informed by the Data Protection Officer in writing if there will be any deviation from the 30 day timeframe due to other intervening events.

Review of Information

The Data Protection Officer will contact and ask the relevant department(s) for the required information as requested in the DSAR. This may also involve an initial meeting with the relevant department to go through the request, if required. The department which holds the information must return the required information by the deadline imposed by the Data Protection Officer and/or a further meeting is arranged with the department to review the information. The Data Protection Officer will determine whether there is any information which may be subject to an exemption and/or if consent is required to be provided from a third party. The Data Protection Officer must ensure that the information is reviewed/received by the imposed deadline to ensure the 30 calendar day timeframe is not breached. The Data Protection Officer will ask the relevant department to complete a "Data Subject Disclosure Form" to document compliance with the 30 day requirement.

Response to Access Requests

The Data Protection Officer will provide the finalized response together with the information retrieved from the department(s) and/or a statement that the Company does not hold the information requested, or that an exemption applies. The Data Protection Officer will ensure that a written response will be sent back to the requestor. This will be via email, unless the requestor has specified another method by which they wish to receive the response (e.g. post). The Company will only provide information via channels that are secure. When hard copies of information are posted, they will be sealed securely and sent by recorded delivery.

Archiving

After the response has been sent to the requestor, the DSAR will be considered closed and archived by the Data Protection Officer

Exemptions

An individual does not have the right to access information recorded about someone else, unless they are an authorized representative, or have parental responsibility.

The Company is not required to respond to requests for information unless it is provided with sufficient details to enable the location of the information to be identified, and to satisfy itself as to the identity of the data subject making the request.

In principle, the Company will not normally disclose the following types of information in response to a Data Subject Access Request:

- Information about other people – A Data Subject Access Request may cover information which relates to an individual or individuals other than the data subject. Access to such data will not be granted, unless the individuals involved consent to the disclosure of their data.
- Repeat requests – Where a similar or identical request in relation to the same data subject has previously been complied with within a reasonable time period, and where there is no significant change in personal data held in relation to that data subject, any further request made within a six month period of the original request will be considered a repeat request, and the Company will not normally provide a further copy of the same data.
- Publicly available information – The Company is not required to provide copies of documents which are already in the public domain.

Data Subject Access Request Refusals
There are situations where individuals do not have a right to see information relating to them. For instance:

- If the information is kept only for the purpose of statistics or research, and where the results of the statistical work or research are not made available in a form that identifies any of the individuals involved.
- Requests made for other, non-data protection purposes can be rejected.

If the responsible person refuses a Data Subject Access Request on behalf of the Company, the reasons for the rejection must be clearly set out in writing. Any individual dissatisfied with the outcome of his/her Data Subject Access Request is entitled to make a request to the Data Protection Officer to review the outcome.

Record Retention Policy

In this policy Keltech has established retention or destruction schedules or procedures for specific categories of records, this is done to ensure legal compliance.

All employees should give special consideration to the categories of documents listed in the record retention schedule below.

Avoid retaining a record if there is no business reason for doing so and consult with the Data Protection Officer if unsure.

Personnel Records		
Record	Retention Period	Basis
Employee applications and resumes	1 Year and 1 Day or where successful, for the duration of the employment plus 3 years from date of termination of employment.	Legal Basis to Execute Contract
Employee offer letters (and other documentation regarding hiring, promotion, demotion, transfer, termination or selection for training)	1 Year and 1 Day or where successful, for the duration of the employment plus 3 years from date of termination of employment.	Legal Basis to Execute Contract and facilitate returning employees and employees seeking training records for new employer (training certificates generally last 3 years).
Records relating to background checks on employees	1 Year and 1 Day or where successful, for the duration of the employment plus 3 years from date of termination of employment.	Legal Basis to Execute Contract
Employment contracts; employment and termination agreements	Duration of the employment plus 3 years from end of calendar year from date of termination of employment.	Legal Basis to Execute Contract
Injury and Illness Incident Reports and related Annual Summaries; Logs of work-related injuries and illnesses	Duration of the employment plus 3 years from end of calendar year from date of termination of employment.	Legal Basis to Execute Contract and Vital Interest to ensure employee safety and wellbeing.
Job descriptions, performance goals and reviews;	Duration of the employment plus 3 years from end of calendar year from date of termination of employment.	Legal Basis to Execute Contract

Written allegations/ complaints	Duration of the employment plus 3 years from end of calendar year from date of termination of employment.	Legal Basis to Execute Contract and Vital Interest to ensure employee safety and wellbeing.
Log and Summary of Occupational Injuries and Illnesses	Duration of the employment plus 3 years from end of calendar year from date of termination of employment.	Legal Basis to Execute Contract and Vital Interest to ensure employee safety and wellbeing.
Injury and Illness Incident Reports and related Annual Summaries; Logs of work-related injuries and illnesses	Duration of the employment plus 3 years from end of calendar year from date of termination of employment.	Legal Basis to Execute Contract and Vital Interest to ensure employee safety and wellbeing.

Payroll Records		
Record	Retention Period	Basis
Employee records with information on pay rate or weekly compensation	7 Years from end of calendar year.	Legal Basis to Execute Contract
Employee tax records	7 Years from end of calendar year.	Legal Basis to Execute Contract
Time reports	7 Years from end of calendar year.	Legal Basis to Execute Contract
Superannuation / Pension/ Retirement records	7 Years from end of calendar year.	Legal Basis to Execute Contract
Payroll registers (gross and net)	7 Years from end of calendar year.	Legal Basis to Execute Contract
Clock in times; wage rate tables; pay rates; work and time schedules; earnings records; records of additions to or deductions from wages; records on which wage computations are based	7 Years from end of calendar year.	Legal Basis to Execute Contract

Accounting & Finance Records		
Record	**Retention Period**	**Basis**
Accounts Payable and Receivables ledgers and schedules	7 Years from date record was made.	Legal Basis
Annual audit reports and financial statements	Permanent	Legal Basis
Bank statements, cancelled checks, deposit slips	7 Years from date record was made.	Legal Basis
Business expense records	7 Years from date record was made.	Legal Basis
Details of cheques/stubs	7 Years from date record was made.	Legal Basis
Electronic fund transfer documents	7 Years from date record was made.	Legal Basis
Employee expense reports	7 Years from date record was made.	Legal Basis
General ledgers	Permanent	Legal Basis
Journal entries	7 Years from date record was made.	Legal Basis
Invoices	7 Years from date record was made.	Legal Basis

Website Data Protection Policy

When you visit our internet site, your PC's current IP address, the type of browser you are using, your PC's operating system, and your visits to the pages you view are logged. However, it is neither possible nor our intention to link this information to your personal data.

We take our security responsibilities seriously, employing the most appropriate physical and technical measures, including staff training and awareness. We review these measures on an ongoing basis.

The personal data you submit to us by e-mail (such as your name and contact information) enables us to correspond with you, and it is processed only for the purpose for which you have provided the data.

We do not pass any personal details (including name, address, phone number and email address) provided through this site to third parties.

All of the customer data we collect is protected against unauthorised access and is not supplied to any third party. We do not sell, trade, or rent your personal information to others. We will never disclose your personal data to any third party without your prior express consent unless we are required to do so by law. Personal data submitted to us through our website is stored only until the purpose for which it has been entrusted to us has been fulfilled.

If you need to contact us with questions concerning the collection, processing, or use of your personal data or in regard to disclosure, correction, blocking, or deletion of data, we can be reached either by post or by completing our form on our contact us page. You can also contact these addresses at any time to have the data saved by us checked, changed, blocked, or deleted.

We use a web analytics tool to analyse site usage, how our users arrive at our site, what they do on the site, what browser they are using and on what operating system etc. However, this analytics data is not tied to personally identifiable information.

We use a number of different cookies on our site. If you do not know what cookies are, or how to control or delete them, then we recommend you visit www.aboutcookies.org for detailed guidance.

We operate an 'implied consent' policy which means that we assume you are happy with this usage of cookies. If you are not happy, then you should either not use this site, or you should delete cookies having visited the site, or you should browse the site using your browser's anonymous usage setting (called "Incognito" in Chrome, "InPrivate" for Internet Explorer, "Private Browsing" in Firefox and Safari etc.)

We use Google Analytics to understand how the site is being used in order to improve the user experience. User data is all anonymous with this service.

Should you require any further information please do not hesitate to contact us.

Email, Internet and Social Media Policy

Policy Statement

Keltech is committed to ensuring email, internet, social media and computer usage that protect the company and its interests while also ensuring dignity at work for all employees.

Purpose

The purpose of this policy is to outline the procedure for the use of email, internet, social media and computer resources within Keltech

Scope

All employees of Keltech

Responsibilities

- Employees are required to familiarise themselves with and adhere to the provisions outlined in this policy.
- Supervisors are responsible for ensuring all employees comply with the terms of this policy.
- The HR Coordinator is responsible for ensuring consistent application of this policy and providing advice and support to supervisors regarding the monitoring and management of this policy.

General Principles

- The following list gives examples of conduct that is prohibited in the use of the company's computer systems. This list should not be considered to be exhaustive.
    - Violation of copyright laws.
    - Using the computer or network facilities for unauthorised profit or gain.
    - Posting, transferring, downloading, viewing or linking to material that is offensive, abusive, threatening or harassing images or material. This includes entertainment software, games images etc.
    - Unauthorized access to another person's files or messages.
    - Use or transfer of unauthorised or unlicensed material.
- Personal use of the internet without authorisation.
- Keltech reserves the right and intends to monitor email and internet usage.
- This policy is not exhaustive. In situations that are not expressly governed by this policy, you must ensure that your actions are at all times appropriate and consistent with your responsibilities towards the company.

Email

- The email system is to be used solely for the purposes of Keltech and not for personal purposes of employees. Personal emails should only be sent in exceptional circumstances.

- E-mails should be regarded as potentially public information which carry a heightened risk of liability for the sender, the recipient and the company.
- An e-mail should be regarded as written formal correspondence, the recipients of which may be much wider than the sender intended, hence any defamatory or inappropriate remarks have serious consequences as can any indirect innuendo.
- E-mail has the same permanence and legal status as hard copy. Employees must ensure that the same professional standards that apply to other written documentation are also applied to e-mails, including levels of confidentiality. E-mails to outside organisations have the same power to create binding contracts as hard copy documents.
- When communicating using e-mail it is important for employees to be respectful and clear as if you were writing a formal business letter. Each mail sent should identify the subject matter. If the mail is private it should be identified as such.
- Particular care should be taken when sending confidential or sensitive information internally or to parties outside of the company. Please ensure to password protect any confidential or sensitive attachments.
- Users must not send messages, including attachments, which are abusive, threatening, defamatory, offensive, harassing, obscene, racist, sexist or other inappropriate remarks whether in written, cartoon form or otherwise.
- Users must not partake in or promote the sending or distribution of chain email messages or send unnecessary files which would adversely affect computer and network resources.
- If an employee receives any offensive, unpleasant, harassing or intimidating messages via e-mail they should contact their supervisor immediately.

E-mail messages/attachments can carry computer viruses which are particularly harmful to the company computer systems. Hence, it is critical that the Purchasing Manager is contacted if an employee receives an e-mail from an unknown sender or an e-mail which may contain a virus. Under no circumstances should an employee respond to spam emails.

Internet

- Access to the internet is solely for business purposes during working hours. Access during breaks is permitted and use outside of working hours is allowed with the agreement of your supervisor. Where permission is granted usage must at all times be in line with the terms of this policy.
- There is no quality control process on the internet and a considerable amount of information published on the internet is outdated, inaccurate or deliberately misleading. All information obtained from the internet should be considered with caution until confirmed by a reliable source.
- Employees must at all times respect copyright and intellectual property rights of information which they encounter on the internet. Proper credit to the source of information used for company purposes must be given.
- Internet access may potentially provide employees with access to material unsuitable for the work place. It is strictly against Company policy for employees to download, view, send and knowingly receive any material that may potentially be considered:
- Offensive (for example: discriminatory on the grounds of sex, age, religion, race, colour, sexual orientation, ethnic or national origin or disability. This includes jokes, text, pictures, or such materials that have the potential to cause offence)
- Intimidatory (for example: threatening text or picture)

- To leave Keltech open to criminal or civil action (for example: potentially illegal information, libellous material, breach of copyright law and material likely to cause offence).

Social Media

- Social media refers to the use of web based and mobile applications for social interaction and the exchange of user-generated content. Social media channels include Facebook, Twitter, Linkedln, You Tube, Flickr, Blogs, review sites, forums and any similar online platforms.
- Keltech is committed to utilising social media to enhance its profile and reputation, to listen and respond to customer opinions and feedback, and drive revenue, loyalty and advocacy. We encourage employees to support our activities through their personal social networking channels while adhering to the guidelines outlined in this policy.
- Employees are encouraged to become fans and followers of the company's profile and to share company generated content within their personal networks. However, the company's channels are administered by designated people only and all official content must be approved and distributed by them.
- Access to social media sites for personal purposes is not permitted during working hours. Access during breaks is permitted and use outside of working hours is allowed with the agreement of your supervisor. Where permission is granted usage must at all times be in line with the terms of this policy.
- When using social media sites employees should always be mindful of what they are posting, who can see it, and how it can be linked back to the company and work colleagues. Behaviour and content that may be deemed disrespectful, dishonest, offensive, harassing or damaging to the company's interests or reputation are not permitted. Employees must not disclose private and confidential information about the company, its employees, clients, suppliers or customers on social networks.
- Keltech reserves the right to utilise for disciplinary purposes any information that could have a negative effect on the company or its employees, which management comes across in regular internet monitoring, or is brought to their attention by employees, customers, members of the public etc.

Anti-Virus and Data Protection

- An employee who suspects a PC / laptop has been infected with a virus must notify their supervisor immediately.
- Keltech network antivirus system and spam arrest are regularly monitored.
- All data stored on the Company's equipment is the property of Kel–Tech Engineering Ltd.
- Employees should not omit to do anything which may lead to any information held on IT Systems to be lost, disclosed or accessed by third parties.
- Maintaining password privacy is the responsibility of each individual employee and consequently employees are responsible for any abuses taking place using their name and password.
- All critical data on laptops or local hard drives must be backed up onto the Network or a removable device on a regular basis. This is the responsibility of the user.

Computer Equipment

- Computer equipment must be treated with care. Any damage must be reported to your supervisor or the Purchasing Manager.
- In order to maximise the efficiency of the computer network and minimise the risk of viruses, PCs may only be loaded with Company approved software in conjunction with the Purchasing Manager.
- All documents / files copied to external devices (USB storage/disks) are covered by the general confidentiality obligations which apply to all aspects of your employment.
- All PCs / laptops will be scanned periodically to complete a hardware and software audit.
- Uploading of non licensed software (i.e. pirate copies) to any of Keltech's computer equipment is strictly prohibited. If you are in any doubt you should contact the Facility/ Utility Manager.
- Any unauthorised software that has been installed will be removed.
- Non–employees of Kel–Tech Engineering, including partners and children are not permitted to use the Company's equipment without prior permission.
- Company laptops should not be left in unattended vehicles.
- Company laptops should be kept as hand luggage when travelling.
- Any act or misuse of computer equipment may be found as misconduct and may lead to disciplinary procedure.

Breach of the Policy

- Any breach of this policy may lead to disciplinary action up to and including dismissal.

Data Request Form

The General Data Protection Regulations (GDPR) 2016 provides you, the data subject, with a right to receive a copy of the data/information we hold about you or to authorise someone to act on your behalf. Please complete this form if you wish to see your data. You will also need to provide proof of your identity. Your request will be processed within 30 calendar days upon receipt of a fully completed form and proof of identity.

Proof of identity:

We require proof of your identity before we can disclose personal data. Proof of your identity should include a copy of a document such as your birth certificate, passport, driving licence, official letter addressed to you at your address e.g. bank statement, recent utilities bill. The document should include your name, date of birth and current address. The proof provided will be destroyed immediately once the request has been verified.

Administration fee:

Keltech's policy is not to charge for Subject Access Requests.

Section1

Please fill in your details (the data subject). If you are not the data subject and you are applying on behalf of someone else, please fill in the details of the data subject below and not your own.

Title:
Surname:
First Name:
Date of Birth:
Address:
Telephone No:

I am enclosing a copy of the following as proof of identity: Driving License: _____

Passport: _____ Utility Bill:_____

Personal Information

If you want to know what information is held in specific record's please indicate in the box below. Please tell us if you know in which capacity the information is being held, together with any dates you may have.

Details:

Data Subject Declaration: I certify that the information provided on this form is correct to the best of my knowledge and that I am the person to whom it relates. I understand that Keltech is obliged to confirm proof of identity/authority and it may be necessary to obtain further information in order to comply with this subject access request.
Name:
Signature:
Date:

I wish to:

Receive the information by post: _____

Collect the information in person: _____

Go through the information with a staff member: _____