DATA PROTECTION POLICY

1. Introduction

Crossfields Institute needs to retain and process certain data in order to enable the efficient running of the business. This includes certain personal data on our employees, customers, clients and other associates of the business. We are committed to the principles of Data Protection legislation and this policy sets out our obligations and the requirements we have of our employees.

Crossfields Institute has appointed Lou Doliczny as Data Controller, she will be responsible for monitoring our compliance with data protection principles as well as the effectiveness of this policy.

2. Data Protection Principles

Under Data Protection legislation there are certain responsibilities in relation to personal data held on computers and also certain manual records where they form part of a structured filing system. Under the regulations, all personal data is subject to the 'eight data protection principles'. All employees must be aware of and act in accordance with the principles. These are that personal data:

- must be processed fairly and lawfully
- must be obtained for lawful purposes
- must be adequate, relevant and not excessive
- must be accurate and where necessary kept up to date
- must not be kept longer than necessary
- must be processed in accordance with the rights of employees
- must be safeguarded against unauthorised or unlawful processing and against accidental loss, damage or destruction
- must not be transferred to a country outside the European Economic Area

2.1. Employee Obligations

All employees are required to take practical steps to comply with the principles, including keeping a clear desk outside working hours, ensuring personal data is never left visible or unattended on a desk, photocopier or computer screen.

You should never disclose personal information about another member of staff, a customer, supplier or client.

During the course of your work you are likely to have access to information which is private or confidential to the Company, fellow or former employees, clients, customers or suppliers. You have a responsibility for the preservation of the confidentiality and integrity of information used during the course of your work.

If, as part of your role, you collect personal information about employees or other people such as clients, suppliers or colleagues, you must comply with this policy including the eight data protection principles. You must also comply with the following guidelines at all times:

- Do not disclose confidential personal information to anyone except the data subject, unless the data subject has given their explicit prior written consent to this
- Ensure you verify the identity of the individual and the legitimacy of the request before releasing any personal information
- If you receive a request for personal information about another employee, you should forward this to the HR liaison person who is responsible for dealing with such requests
- Ensure any personal data you hold is kept securely and is not seen by unauthorised persons
- Ensure that, when working on personal information as part of your job duties when away from your workplace, you continue to observe the terms of this policy, in particular in relation to data security
- Ensure that hard copy personal information is disposed of securely
- Take practical steps to support the adherence to the principles, for example keeping passwords separately from laptops and phones, using a strong password and not sharing your password with others

Remember that compliance is your personal responsibility

Please note that failure to follow the above obligations or comply with the Data Protection principles may be considered a disciplinary matter.

2.2. Crossfields Institute's Obligations

Crossfields Institute holds personal data about you. We need to process your personal data to carry out our legal duties under the employment contract including payroll and benefits administration and to ensure we can carry out our general business and HR activities.

The publishing of information such as an annual report, marketing material, etc. which contains employee information is not prohibited, but the following guidelines should be followed. Information about employees should only be published where:

- there is a legal obligation to do so, or
- the information is clearly not intrusive, or
- the individual has consented to the disclosure, or
- the information is in such a form that it does not identify individuals.

Where the employee gives their consent they should be made aware of the extent of information that will be published, how it will be published and the implications of this.

Under Data Protection legislation the 'reason' for sickness absence is classified as 'sensitive personal data' and as such must not be disclosed without the express consent of the individual. As a consequence, the reason for illness will only be disclosed to the individual's line manager. There should be no discussion or disclosure of the reason for sickness except between the individual, line manager and member of the Chief Executive Officer with responsibility for HR.

Anyone whose personal data is being processed by the Company has certain rights in relation to their personal data. In practice, what this means is that individuals have the right, on written request and within a month, to:

- be told what personal data is being processed, why it is being processed, where it came from and to whom it may be disclosed
- access that data in an intelligible form
- ask to rectify the data if inaccurate
- ask for the data to be erased
- restrict processing
- data portability (in certain circumstances); and
- not to be subject to automated decision-making, for example in recruitment selection

3. Further information or queries

For further information, or in the case of any queries over this policy or a particular matter of data protection, please consult the Data Controller.

Policy last reviewed: September 2020
Next revision date: September 2021
Reviewed by: Lou Doliczny, Data Controller

Appendix - Retention of personal data by Crossfields Institute

Crossfields Institute is required to retain personal data for a variety of purposes. We will not retain data for any longer than is required by a legitimate purpose.
The table below sets out the data that we retain, for how long and why.

Category of data	Location of storage	Retention period	Criteria to determine the retention period
Individual learner details (names, date of birth, gender, unique learner number)	Mercury *(Crossfields Institute management information system)*	Indefinitely, unless requested to remove	We retain this data in case there is a need for a learner/employer/education provider to request confirmation of certification or replacement certificates
Learner application forms (Crossfields Institute International)	Secure server and locked filing cabinet for paper forms	Duration of the course	This provides information that we may need to access to contact the student or make specific arrangements for them
Assessment evidence (including RPL records)	Secure server, secure online fileshare (eg. Dropbox)	Until learner has qualified and EQA has had an opportunity to review evidence	This evidence is primarily held and shared with Crossfields Institute by approved centres. It must be retained until all quality assurance procedures have been satisfactorily completed.
Assessment & monitoring records - EQA Reports, IQA Reports, Assessment feedback, Attendance/Notes from meetings	Secure server	3 years	This may be required for audit by Ofqual (the regulator). The only personal data should be names and signatures.
Individual learner and staff logins for the virtual learning environment (VLE) – this requires first and last name and email address	www.overtsoftware.com hosts Crossfields Institute VLEs (GDPR compliant)	For the duration of the course and indefinitely thereafter unless removed requested by learner or the course is closed	This allows learners to continue to access resources as long as they are made available.
Mailing list membership (first and last names and email address)	www.mailchimp.com (online email marketing platform) GDPR compliant	Indefinite, receiver can request to opt-out at any time	Consent is required to join a mailing list, and there is always an option to unsubscribe

Employment applicants	Secure server and locked filing cabinet for paper records	6 weeks after applications close	We retain applications for a short period of time, and may ask to retain them for longer if an applicant wishes to be contacted in relation to future employment opportunities
Employee and third party records	Secure server and locked filing cabinet for paper records	7 years from the end of employment or contract	Records held in order to be able to respond meaningfully to employment reference requests or to respond to HMRC requests
Special Category data (sensitive data – e.g. medical records, ethnicity, disabilities, etc)	Secure server – restricted access to data controller and designated data processors	The shortest possible time; context dependent.	We will retain this data in relation to special consideration applications for learners for as long as needed to make a decision. We will retain this in relation to employees for as long as needed to ensure that their health and wellbeing needs at work are met.
Criminal data	Secure server – restricted access to data controller and designated data processors	The shortest possible time; context dependent.	We will retain this data for as short as possible a time, due to its sensitive nature. The only likely context for us to require this data is when a DBS check is required for employees or third party suppliers