# P14 Information Security Policy

## 1. Introduction

**1.1** Everyone has right to ensure their personal information, data is handled, stored, and shared in a confidential, safe, and secure manner. Crosby Management Training Ltd ("Crosby") is an apprenticeship and commercial training provider, specialising in the delivery of apprenticeships and qualifications. During our activities, we will collect, store, and process a range personal data, including some limited sensitive data, about our employers, learners (apprentices), suppliers and other third parties. We recognise that the correct and lawful handling and management of data has an important role to play in maintaining Crosby's professional reputation and enabling Crosby to conduct its business operations successfully. We also note the importance of sharing with employers and when necessary, the ESFA or other professional agencies the personal data we hold about learners (apprentices) if there is a need to do so from a safeguarding perspective.

**1.2** Crosby will collect, evaluate, and store a range of personal information about learners (apprentices) this includes the necessary records of learning (ILR). Personal learning records do contain personal and sensitive data that Crosby processes to manage and monitor the learners (apprentices) progress whilst on their programmes of learning and to comply with the ESFA rules on compliance and funding. Some limited personal data such as names and emails are provided to us directly by employers and our clients, but the personal data that we collect from learners is provided to us by learners (apprentices) their employers directly populated into BUD the secure platform this is used to manage all learners and learning programmes.

**1.3** Crosby will collect, evaluate, and store a range of personal information about other data subjects including employees, associates, third party service providers as required by Law and required through our onboarding processes. Personal data is limited that required to fulfil the role/service being provided.

**1.4** Crosby colleagues (data users) are required to fully comply with this policy when processing, storing, and communicating personal data on our behalf. Any breach of this policy may result in disciplinary action.

## 2. About this Policy:

**2.1** The types of sensitive personal data that Crosby may be required to process include information about current, past and prospective learners (apprentices), employers, employees and others that we work and communicate with. Most personal data is held in one of our three key Cloud based Software platforms: Office 365, Bud Systems or Learning Alchemy). A limited quantity of personal data is held within paper, documented records which is always securely stored when not in use. Whatever the method of storage, all data is subject to defined legal safeguards specified in the Data Protection Act 2018 (the "Act"), the General Data Protection Regulations ("GDPR") and other relevant regulations.

**2.2** This policy and other documents referred to in this policy set 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.

**2.3** This policy does not form part of any Crosby colleagues' contract of employment and may be amended at any time.

**2.4** This policy has been approved by Crosby's appointed Data Protection Officer and sets out rules on data protection and the legal conditions that must be adhered to when we obtain, handle, process, transfer, and store personal data.

## 3. Definition of Data Protection Terminology.

**3.1** **Data** is information which is stored electronically, on a computer, or in various paper-based filing systems.

**3.2** **Data subjects** for the purpose of this policy include all living individuals about whom we hold personal data. A data subjects need not be a UK nationals or resident. All data subjects have legal rights in relation to the security of their personal information.

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

**3.4** **Data controllers** are the Crosby colleagues or organisations which determine the purposes for which, and the way, any personal data is processed. They are responsible for establishing practices and policies in line with the relevant data Acts. Crosby is the data controller of all personal data used in our business for our own commercial purposes.

**3.5** **Data users** are those Crosby colleagues 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.

**3.6** **Data processors** include any Crosby colleagues or organisations that are not data users, however they do process personal data on our behalf of Crosby following our instructions. Employees of dedicated data controllers are excluded from this definition, but it could include suppliers which handle personal data on Crosby's behalf.

**3.7** **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.

**3.8** **Sensitive personal data** 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 identity and orientation. Sensitive personal data relating to a persons protected characteristics can only be processed under strict conditions, including a condition requiring the permission of the person concerned.

## 4. Data Protection Principles:

**4.1** Anyone processing personal data must comply with the seven 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 (data minimisation).
(d) Accurate.
(e) Not kept longer than necessary for the purpose (storage limitation).
(f) Secure (integrity and confidentiality).
(g) Processed in a compliant manner, with those processing such data to be responsible for complying with the GDPR and demonstrating their compliance (accountability).

## 5. Fair and Lawful Processing:

**5.1** The Act is 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.

**5.2** To ensure the lawful protection of data when processing lawfully, data must be processed based on one of the legal grounds set out in the Act. This includes, 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 sensitive personal data is being processed, additional conditions must be met. When processing personal data as data controllers during our business, we will ensure that those requirements are met.

## 6. Processing for Limited Purposes:

**6.1** In the course of our business, we may collect and process the personal data for several reasons including onboarding new employees, clients and services. 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, funding bodies and others).

**6.2** We will only process personal data for the specific purposes set out in our contracts of engagement with data subjects or for any other purposes specifically permitted by the Act. We will notify those purposes to the data subject when we first collect the data or as soon as possible thereafter.

**6.3** Such personal data is processed and securely stored on our virtual learning environment, BUD, and Crosby's IT system, such as Office 365 (Share Point) only accessible by Crosby colleagues.

## 7. Notifying Data Subjects:

**7.1** If we collect personal data directly from data subjects, we will inform them about:

(a) the purpose or purposes for which we intend to process that personal data.
(b) the types of third parties, if any, with which we will share or to which we will disclose that personal data; and
(c) the means, if any, with which data subjects can limit our use and disclosure of their personal data.

**7.2** If we receive personal data about a data subject from other sources, we will provide the data subject with this information as soon as possible thereafter.

**7.3** We will also inform data subjects whose personal data we process that Crosby is the data controller with regards to that data.

## 8. Adequate, Relevant and Non-excessive Processing:

**8.1** We will only collect personal data to the extent that it is required for the specific purpose notified to the data subject.

## 9. Accurate Data:

**9.1** We will ensure that personal data we hold is accurate and kept up to date. We will check the accuracy of any personal data at the point of collection and at regular intervals afterwards. We will take all reasonable steps to destroy or amend inaccurate or out-of-date data.

## 10. Timely Processing:

**10.1** We will not keep personal data longer than is necessary for the purpose or purposes for which they were collected. We will take all reasonable steps to destroy, or erase from our systems, all data which is no longer required.

## 11. Processing in Line with Data Subjects' Rights:

**11.1** We will process all personal data in line with data subjects' rights, in particular their right to:
(a) Request access to any data held about them by a data controller (see also *Clause 15.*).
(b) Prevent the processing of their data for direct-marketing purposes.
(c) Ask to have inaccurate data amended (see also *Clause 9.*).
(d) Prevent processing that is likely to cause damage or distress to themselves or anyone else.

## 12. Data Security:

**12.1** We will process all personal data we hold in accordance with data security requirements **OR** take appropriate security measures against unlawful or unauthorised processing of personal data, and against the accidental loss of, or damage to, personal data.

**12.2** We will put in place procedures and technologies to maintain the security of all personal data from the point of collection to the point of destruction. Personal data will only be transferred to a data processor if they agree to comply with those procedures and policies, or if they put in place adequate measures themselves that Crosby has been assured are appropriate and meet our standards.

**12.3** We will maintain data security by protecting the confidentiality, integrity, and availability of the

personal data, defined as follows:

**(a) Confidentiality** means that only people who are authorised to use the data can access it.
**(b) Integrity** means that personal data should be accurate and suitable for the purpose for which it is processed.
**(c) Availability** means that authorised users should be able to access the data if they need it for authorised purposes. Crosby will use the built-in security options and settings of the cloud-based platforms that we use such as BUD Systems and Office 365 (Share-Point) to segregate access to data even amongst Crosby colleagues on a 'need to know/use' basis.

**12.4** Security procedures include:

**(a) Entry controls.** Anyone who is not recognised as an employee of Crosby seen in entry-controlled areas should be reported.
**(b) Secure lockable desks and cupboards.** Desks and cupboards should be kept locked if they hold confidential information of any kind. (Personal information is always considered confidential).
**(c) Methods of disposal.** Paper documents should be shredded. Digital storage devices in office spaces, including home offices, should be physically destroyed when they are no longer required.
**(d) Equipment.** Data users must ensure that individual monitors do not show confidential information to passers-by and that they log off from their PC when it is left unattended and/or have an automated screen saver set up those kicks in after an appropriate short period of time.

## 13. Transferring Personal Data to a Country Outside the EEA:

**13.1** Crosby will not normally transfer personal data that we hold outside of the European Economic Area ("EEA"), In cases where we do have to, we will ensure that one of the following conditions applies:

(a) The country to which the personal data are transferred ensures an adequate level of protection for the data subjects' rights and freedoms.
(b) The data subject has given his consent.
(c) The transfer is necessary for one of the reasons set out in the Act, including the performance of a contract between us and the data subject, or to protect the vital interests of the data subject.
(d) The transfer is legally required on important public interest grounds or for the establishment, exercise, or defence of legal claims.
(e) The transfer is authorised by the relevant data protection authority where we have adduced adequate safeguards with respect to the protection of the data subjects' privacy, their fundamental rights and freedoms, and the exercise of their rights.

**13.2** Subject to the requirements in Clause 12.1 above, personal data we hold may also be processed by colleagues operating outside the EEA who work for Crosby or one of our suppliers. That Crosby may be engaged in, among other things, the fulfilment of contracts with the data subject, the processing of payment details and the provision of support services.

## 14. Disclosure and Sharing of Personal Information:

**14.1** We may also disclose personal data we hold to third parties:

(a) if we sell or buy any business or assets, in which case we may disclose personal data we hold to the prospective seller or buyer of such business or assets; and

(b) if we or substantially all our assets are acquired by a third party, in which case personal data we hold will be one of the transferred assets.

**14.2** If we are under a duty to disclose or share a data subject's personal data to comply with any legal obligation, or to enforce or apply any contract with the data subject or other agreements; or to protect our rights, property, or safety of our employees, customers, or others. This includes exchanging information with other companies and organisations for the purposes of fraud protection and credit risk reduction.

**14.3** We may also share personal data we hold with selected third parties for the purposes set out in specific contracts.

## 15. Dealing with Subject Access Requests:

**15.1** Data subjects must make a formal request for information we hold about them. This must be made in writing. Employees who receive a written request should forward it to their Line Manager **and** the Crosby Data Protection Officer, Thomas Bartlett, immediately.

**15.2** When receiving telephone enquiries, we will only disclose personal data we hold on to 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 where their identity cannot be checked.

**15.3** Our employees will refer a request to their Line Manager **OR** the Data Controller for assistance in difficult situation. Employees should not be intimidated into disclosing personal information.

## 16. Duration of Data Processing:

**16.1** Data is to be processed during delivery of an apprenticeship or training programme. Upon completion of any apprenticeship programme, Crosby will meet its obligations towards the Education and Skills Funding Agency (EFSA), personal data will be archived for ten years and then securely deleted. Employee data is held for the durations as required in law by HMRC or other bodies requiring access to this information in line with legislation.

**16.2** Data processed relating to employees, associates, subcontractors, employers and any other group as identified through our processing agreements are held for no longer than required by legislation and individuals will be notified of retention periods through accompany contracts/documentation.

## 17. Complaints:

**17.1** Should data subjects have any complaints; they are advised to refer to Crosby's Complaints Policy and follow the procedure accordingly.

**17.2** Key points of contact regarding data protection enquiries and complaints:

Thomas Bartlett (Chief Operating Officer) – tom@crosbytraining.co.uk

## 18. Changes to this Policy:

**18.1** Crosby reserves the right to change this policy at any time. Where appropriate, we will notify data subjects of those changes by mail or email.

## 19. Colleague Training:

**19.1** All colleagues are required to read and sign to say they understand our data protection policy and subsequent processing arrangement during their induction when starting employment with Crosby.

**19.2** All colleagues' contracts of employment feature specific clauses noting that serious breaches of data protection policies and legislation can amount to dismissal.

**19.3** All colleagues receive annual training linked to their roles and responsibilities relating to data protection, anti-corruption and bribery and must complete this as mandatory CPD on an annual basis frame. This is monitored by the Crosby Quality Manager.

**19.4** Colleagues will complete further Training linked to data protection & data security if it is seen as appropriate for this to be done so sooner than the annual refresher, by a member of the senior management team.

**Paul Cadman: Chief Executive:**

**Author: Tom Bartlett.**
**Edition No: 002**
**Policy No: P14**
**Review Date: 15.10.2024**
**Date of next review: 15.10.2025**