

Data Protection Policy – UK-GDPR

Contents:

- 1 General Statement of the Academy's Duties and Scope
- 2 Definitions
- 3 Accessibility of this document.
- 4 Data Protection Controller and Data Protection Officer
- 5 The Principles
- 6 Personal Data
- 7 Data Security
- 8 Rights of the Data Subject
- 9 Processing of Personal Data
- 10 Sensitive Personal Data
- 11 Criminal Convictions and Offences
- 12 Rights of Access to Information (Subject Access Request or 'SAR')
- 13 Exemptions
- 14 Accuracy
- 15 Enforcement
- 16 External Processors and Controllers
- 17 Secure Destruction
- 18 Retention of Data
- 19 Data Loss Events

Policy Owner	Director sign off	Details of update	Date of Update	Version number
Jason Timms	Lucy Agnew	Policy Development	29/05/18	1
Jason Timms	Lucy Agnew	Policy review and update	12/01/20	2

Jason Timms	Lucy Agnew	Policy Brexit review and Update	12/03/21	3
Jason Timms	Lucy Agnew	Policy review and update	17/03/22	4

1. General Statement of Reflections Duties and Scope

Reflections is required to process relevant personal data regarding members of staff, Learners, applicants, emergency contacts, volunteers, clients, tenants and employers and shall take all reasonable steps to do so in accordance with this policy. Reflections does not sell personal data and only purchases data for legitimate business reasons.

2. Definitions

- “Reflections Training Academies” is the training division of Reflections Group. It includes Next Level Training and additionally covers any contracted subcontractors.
- “Learners” is all persons studying and training with Reflections Training Academies.
- “All Staff” is all staff or employees of the Reflections group, including those on temporary or part time contracts and volunteers.
- “Emergency contacts”, includes the contact details of a parent, carer or custodian to be contacted in case of emergency situation with relevant learner or staff member.
- “employers” is all partner’s employers who engage in delivery of Reflections training programmes inclusive of work experience placements.
- “clients” is all persons who attend a Reflections salon or Training Academy for hairdressing or Barbering services
- “Data Subject”, is a living natural individual who is the subject of the personal data
- “Tenants” are individuals or companies that rent Reflections group properties

3. Accessibility of this document.

This policy is written using clear and plain language and is considered as age appropriate (Age 16 and above) for the accessibility of all data subjects of Reflections. a copy of this document will be posted on The Reflections Training Academy Moodle E-learning platform, Reflections salon division, Reflections Training and Next Level Training Websites

4. Data Protection Controller and Data Protection Officer

Reflections has appointed the **Director of Next Level Training** as the Data Protection Controller (DPC), and the Senior Manager Safeguarding / Prevent (DSL) as Data Protection Officer (DPO) who will endeavour to ensure that all personal data is processed in compliance with this Policy and the Principles of current Data Protection Legislation, currently the Data Protection Act 2018. The Protection of Freedoms Act 2012 is also

relevant to parts of this policy. The Academy is exempt from requests made under the Freedom of Information Act 2000.

5. The Principles

The Reflections Training Academies shall comply with the Data Protection principles contained in the legislation to ensure all data is: -

- Fairly and lawfully processed in a transparent manner.
- Processed for a legitimate purpose.
- Adequate, relevant and not excessive.
- Accurate and up to date.
- Not kept for longer than necessary.
- Processed in accordance with the data subject's rights.
- Processed securely.

6. Personal Data

Personal data covers both facts and opinions about an individual where that data identifies an individual. For example, it includes information necessary for employment such as the member of staff's name and address, their right to work in the UK and details for payment of salary or a learner's programme eligibility, attendance records and programme progress. Personal data may also include sensitive personal data as defined in the legislation. The data collected is explained in greater detail within the relevant division privacy policy

7. Data Security and storage

The organisation will take appropriate technical and organisational steps to ensure the security of personal data. All staff will be made aware of this policy and their duties under the legislation. Reflections and therefore all staff, learners, employers and any other stakeholder are required to respect the personal data and privacy of others and must ensure that appropriate protection and security measures are followed to ensure the unlawful or unauthorised processing of personal data and against the accidental loss of, or damage to all personal data. Violations of this policy by staff may be treated as misconduct or gross misconduct in line with the Reflections company disciplinary procedure. An appropriate level of data security must be deployed for the type of data and the data processing being performed and necessary and appropriate data security systems are in place inclusive of Cyber Essentials the Government backed scheme that protects against a whole range of the most common cyber attacks. Personal data must be stored in appropriate company approved systems and should be encrypted when transported offsite. Some personal data however may be appropriate for publication or limited publication within the company, therefore having a lower requirement for data security, for example learner successes and awards, learner work, salon news articles.

8. Rights of the Data Subject

UK-GDPR expands the rights of the data subject over previous legislation, specifically data subjects have:

1. The right to be informed.
2. The right of access.
3. The right to rectification.
4. The right to erasure.
5. The right to restrict processing.
6. The right to data portability.
7. The right to object.
8. Rights in relation to automated decision making and profiling.

This policy and the published Privacy policy are part of these rights. If you wish to exercise or receive a request to exercise any of these rights, with the exception of the right to access, please contact the company department processing that information in the first case or email gdpr@reflectionstraining.co.uk. Information on the right of access and how to exercise that are specifically detailed in this policy. Not all rights are applicable to all personal data, and may depend on the lawful basis that personal data is being processed under.

9. Processing of Personal Data

The Academy maintains a Privacy Policy which details personal information processed and the legal basis for processing that data. The current version can be viewed on all company websites; a copy can also be requested to be viewed at the relevant business building. Reflections processes some personal data for purposes considered direct marketing. Data subjects have the right to withdraw consent to these activities these requests should be via a SAR request to gdpr@reflectionstraining.co.uk.

10. Sensitive Personal Data

Reflections may, from time to time, be required to process sensitive personal data especially in HR and training functions. Sensitive personal data includes data relating medical information, age, gender, religion, race, sexual orientation, safeguarding information. This information is gathered and processed as a legal obligation within the company's function.

11. Criminal Convictions and Offences.

The Reflections does not maintain registers of or process data on Criminal Convictions and offences, other than is required for the safeguarding purposes within its training divisions. Specifically, Enhanced DBS checks are required for all regulated activity staff within the training division. Where convictions or adverse findings are present that data is used as part of a staff recruitment risk assessment and recorded with in central register system Sentry.

12. Rights of Access to Information (Subject Access Request or 'SAR')

Data subjects have the right of access and removal of their Personal data held by Reflections, subject to the provisions of current Data Protection legislation. Any data subject wishing to access their personal data should put their request in writing to the DPC or DPO via gdpr@reflectionstraining.co.uk. Reflections will endeavour to respond to any such written requests as soon as is reasonably practicable and, in any event, no longer than one month for access to personal data. The information will be made available to the data subject as soon as is reasonably possible after it has come to the Academy's attention and in compliance with the relevant legislation. Proof of identity is required before any information will be made available. Only the DPC or DPO can authorise a Subject Access Request. Any other staff receiving such a request **MUST** immediately pass it to the DPC / DPO for processing or refer the person making the request to the DPC / DPO

Where Reflections receives a Data Subject Request (or purported Data Subject Request) in relation to processing their data (submission of learner data): receives a request to rectify, block or erase any Personal Data processed through the submission of learner data; receives any other request, complaint or communication relating to their ESFA data processing obligations under the Data Protection Legislation or receives any communication from the Information Commissioner or any other Regulatory Body in connection with Personal Data processed under the ESFA Contract; receives a request from any third Party for disclosure of Personal Data where compliance with such request is required or purported to be required by Law then notification in such cases should be given via the ESFA Contract Manager;

13. Exemptions

Certain personal data or obligations are exempted from the some of the provisions of the Data Protection legislation which includes matters such as processing for National Security and Public Security, the prevention or detection and prosecution of criminal offences. The above are examples only of some of the some of the exemptions under the legislation. Any further information on exemptions should be sought from the DPC or DPO or via the Information Officers website <https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/>

14. Accuracy

The Reflections will endeavour to ensure as far as reasonably practical that all personal data held in relation to all data subjects is accurate. Data subjects must notify the relevant salon or academy of any changes to information held about them.

15. Enforcement

If an individual believes that the Reflections has not complied with this policy or acted otherwise than in accordance with data protection legislation notify the DPC or DPO via gdpr@reflectionstraining.co.uk.

16. External Processors and Controllers

The Reflections will ensure that data processed by external processors, for example, service providers and Cloud services including storage, web sites are compliant with this policy and the relevant legislation. All external processors and controllers must be listed in the data processing register.

17. Secure Destruction

When data held in accordance with this policy is destroyed, it will be destroyed securely in accordance with best practice at the time of destruction.

18. Retention of Data

The Reflections may retain data for differing periods of time for different purposes as required by statute or best practice. Statutory obligations, legal processes and enquiries may also direct the retention of certain data. The Reflections Training Academies may store some data for predetermined periods as set out by contractual government requirements such as registers, photographs, exam results, achievements indefinitely in its archives

19. Data Loss Events

Reflections has in place Protective Measures, which are appropriate to protect against Data Loss Events.

In incidents of Data Loss leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data then an assessment as to whether this poses a risk to people. Consideration to the likelihood and severity of the risk to people's rights and freedoms, following the breach. When this assessment has been made, if it's likely there will be a risk then the ICO must be notified via 0303 123 1113 within 72 hours; Where a significant cyber incident occurs this may also need to be reported to the National Cyber Security Centre. Either of these scenarios would also need to be reported to the ESFA contract Manager

Contacts and Representatives.

The DPC and DPO can be contacted in writing via the published main Academy address. The DPO can be contact via email at gdpr@reflectionstraining.co.uk