



Genna Rose

HAIR & BEAUTY ALTERNATIVE PROVISION

A place to learn, grow & thrive

Date protection & GDPR Policy

2025-2026

Statement of Policy

Genna Rose Training Academy needs to collect and use certain types of information about learners, their families, employees and with whom it deals, in order to perform its functions. This includes information on current, past and prospective employees, learners, persons with parental responsibility, suppliers, customers, service users and others with whom it communicates. Genna Rose Training Academy is required by law to collect and use certain types of information to fulfil its statutory duty and to comply with legal requirements.

The Head of Provision is responsible for data and ensuring the academy is GDPR compliant. Any breaches should be reported to the Head of Provision in the first instance as Data Controller.

This policy should be read in conjunction with 'Children and 'UKGDPR' at <https://ico.org.uk>

Policy Aims

This policy outlines the Academy's arrangements to access personal information by learners, persons with parental responsibility, public and employees in accordance with the UK General Data Protection Regulation (UKGDPR) and the Data Protection Act 2018 and PECR Privacy and Electronic Communication Regulation.

This policy will be communicated to all employees and is accompanied by notes of guidance. This policy will be published to employees through the academy's website.

This policy applies to all personal information held by the Academy irrespective of ownership. Personal information is defined for the purposes of this policy as being any information from which an individual can be identified (including computer storage, documents, photographs, CCTV images, voice etc).

This policy applies to information held by academy, irrespective of ownership, which can identify an organisation and the communication of this information.

Policy Objectives

This policy outlines Academy's approach to ensuring all employees effectively process and manage personal information within set standards, to protect the privacy of individuals and organisations, to comply with the principles and requirements of UKGDPR and other relevant legislation. All employees complete training on procedures that comply with UKGDPR, when handling personal information about learners, parents, visitors, clients, contractors and employees.

This policy should be complied with for personal information relating to all individuals whether deceased or living.

The policy and guidelines cover requests for information for their own personal data. Such requests, defined as subject access requests (SAR's) should be handled in accordance with this policy, in compliance with UKGDPR. (A definition of terms is available at Appendix A).

- To promote the effective, consistent and legal processing of personal information by defining a personal information handling policy.
- To ensure that all employees are aware of their responsibilities in relation to the processing of personal information and to the law surrounding its use.

- To ensure that all employees are aware of the consequences of the misuse or abuse of personal information.
- To establish and maintain trust and confidence in the Academy's ability to process personal information.
- To ensure compliance with post Brexit legislation, guidance and standards relating to the handling of personal information.

Monitoring and Review

The policy and guidelines will be reviewed when necessary to take into account changes in legislation and to ensure that they remain timely and relevant. Any changes will be publicised through the Information Commissioners Office (ICO) and normal communication channels.

The effectiveness of the policy will also be assessed through the monitoring of requests for personal information, the Academy's responses to these, and complaints. These events will be collated into an annual report. Where issues of concerns arise, the Information and Security Officer (ISO) will be approached. The policy will be published on the Academy's website and hard copies will be provided upon request.

Procedure

The Academy regards the lawful and correct treatment of information as critical to successful operations and to maintaining confidence between those with whom it deals. It is essential that it treat information lawfully and correctly and with express permission from the Head of Provision.

The purpose of the UKGDPR is to protect the rights and privacy of living individuals. It regulates the processing of personal information including obtaining, holding, use or disclosure of such information. It places obligations on those who record and use personal information and gives rights to those whose information is being processed.

Processing Information

The processing of information is defined as encompassing everything that we do with information including the sharing, transferring or disclosing of information to another organisation or internally. This includes the use of social media, information can only be shared, transferred or disclosed with the express permission of the Head of Provision or where this information disclosure is in accordance with the law.

Personal information must be processed in accordance with the six principles under the UKGDPR unless an exemption applies.

1. Employees must respect information that they have access to and treat it in the manner in which they would expect their personal details to be treated.
2. Employees must have regard and respect for the privacy of learners, person with parental responsibility and employees and process their information accordingly.
3. Access to information must be accepted by all, to be a need and a right to basis.
4. Personal information should be deleted and disposed of under principles of UKGDPR.
5. Personal information will be held securely and accessible only by those with a need and a right to know. The Head of Provision is responsible for ensuring that personal information held at The Academy is surrounded by appropriate security, i.e. relevant to the sensitivity of personal information being processed.

Personal information must not be transmitted or transported externally via manual or electronic means without appropriate security. Possible devices (laptops, CD's DVD's USB memory sticks etc) which contain personal information must use adequate security measures e.g. encryption, to protect against losses or access by unauthorised persons. The Data Controller/Head of Provision requests that no identifiable collected information will be accessed by laptops unless encrypted. This is because collected data is the responsibility of the Data Collector/Head of Provision.

Personal information must be disposed of safely and securely when it has reached its shelf life. Information will not be passed on to any third party unless any one or more the following apply (principles of UKGDPR):

- Explicit consent from both the Head of Provision and the Data subject is obtained.
- The organisation requesting the information has a legal right to the information (e.g. police investigating crime)
- It is a requirement of law
- It is to comply with a court order
- It is necessary to provide educational services
- The Academy believes it is in the subjects own interest
- The Academy believes it is in the overall public interest and in a particular instance this is judged to outweigh the other considerations.

At the point of collection and disclosure, the data subject will be informed of the purposes for which the information is being collected, processed or disclosed together with any other relevant details. At this time, where choices are available, the child/young person or persons with parental responsibility or organisation will be given the opportunity to opt out of the information processing arrangements.

The Academy will promote good practice in the sharing of information with its partners, government agencies and departments and other public and private sector organisations. All sharing will comply with the UKGDPR and the current General Information Sharing Protocol (GISP).

- The quality and accuracy of personal information should be relevant to the purpose for which it is to be used.
- The purposes for which personal information is processed in the Academy will be detailed in the academy Data Protection Notification.
- Any changes to purpose must be identified to the ISO who will submit amendments as required.
- Processing of information for a purpose not reflected in the UKGDPR or in the notification must be approved by the ISO.
- Any inaccurate or misleading information will be checked and corrected as soon as the school, learner, parent or organisation brings this to the Academy's attention.
- The rights of data subjects as identified by the UKGDPR 2016, and specifically their right of access to their own personal information will be complied with fully and given appropriate respect and priority.

Data Security and Storage of Records

Personal information must be stored securely, accessible only to those with a legitimate need. The Head of Provision, ensures personal information is protected by appropriate security measures proportionate to the sensitivity of data.

Digital records must be protected by strong passwords, encryption, and access control. Physical records must be stored in locked cabinets or secure storage rooms.

Any portable devices containing personal information (e.g. USB's, laptops) must use encryption and password protection.

Disposal of Records

- Personal information must be securely deleted or shredded when it is no longer needed
- Digital records must be permanently deleted from storage and backup systems.
- Records containing sensitive or special category data must be disposed of via approved destruction methods
- Data must not be deleted or disposed of after a subject access request unless requested by the subject
- The Academy's should ensure data is only returned for the legally required period

Personal Data Breach Procedure

A data breach occurs when personal information is lost, disclosed, or accessed without authorisation.

If a data breach occurs:

1. Identify and contain the breach
2. The individual discovering the breach must report it to the Head of Provision
3. The Head of Provision must assess the severity and determine containment actions

Risk Assessment

1. Evaluate the nature of the data involved (e.g., special category data, financial details, personal identifiers).
2. Assess the potential harm to affected individuals (e.g. identity theft, financial loss, distress).
3. Report the breach
4. If the breach poses a high risk to individuals, it must be reported to the Information Commissioner's Office (ICO) within 72 hours
5. The Academy must notify affected individuals without undue delay if the breach is unlikely to result in serious harm

Investigation and Resolution

1. Document how the breach occurred and identify corrective actions
2. Implement additional security measures to prevent future breaches
3. Review and lessons learned
4. Conduct a post-incident review to identify weaknesses in data security
5. Update policies and train staff to mitigate risks
6. The Subject Access Request procedure

See details on 'Manifestly unfounded and Excessive Requests' September 2019 at www.ico.org.uk

Requests by individuals (or their representative) for copies of their own information must be in writing and supported by significant proof of identity. The following originals (not photocopies) are suggested:

- Passport
- Driving License
- Birth/Marriage Certificate

The need to check and verify the identity of the requester can be particularly important where that person is a child or someone is purportedly making the request on behalf or in respect of child.

Enquirers should make a SARs using the exemplar format as a guide adding exactly what information is required (Appendix B).

In the event of a SARs request, the Head of Provision will prepare and direct all relevant information. This is also to ensure compliance within timescales.

Information must not be disposed of or deleted, after the receipt of a request, unless requested by the subject. Subjects have the right to have incorrect or inaccurate information corrected. Deleting information constitutes a new offense without permission.

SARs will be supplied without undue delay or within one month. Where an investigation of a member of staff has commences and that member of staff has requested a SAR, the processing of the request should be taken as quickly as possible. In the event that a complaint is received regarding a SAR, the complaint will be addressed following the Academy's complaints procedure. Records of proceedings and decisions made will be kept in order to provide for any external review of the complaint by the ICO.

Training

All employees in organisations with over 250 staff require training on UKGDPR and personal information handling. Genna Rose Training Academy does not meet this staffing number.

Security of Personal Data

Unacceptable use includes:

- Unauthorised access to personal information
- Unauthorised disclosure of personal information
- Unauthorised use of personal information, e.g. use of which the data subject has not been informed/consented to as in UKGDPR Law

Employee, client or learner personal information must not be used for:

- An illegal purpose
- Any purpose which is inappropriate in the workplace by virtue of the fact that it may cause embarrassment or distress to another person or may bring the Academy into dispute; or
- Any purpose which is not in accordance with the employee's role or job description.

Employees are required to notify the Head of Provision, if they become aware or suspect that personal information is being misused or handled inappropriately.

Non-Compliance with Legislation & Policy

The Head of Provision is responsible for ensuring that employees' Responses for personal information remain appropriate and are in accordance with this policy and the UKGDPR.

The Head of Provision must ensure that instructions they give to employees, relating to request for personal information and the processing of personal information, comply with UK GDPR.

Employees need to be aware that arrangements need to be in place to avoid parental and visitor contacts with personal information to which they do not have a right.

All employees must be aware of their own obligations with regard to disclosure and the processing of information.

Employees not complying with this policy or legislation will have matters reviewed and may be dealt with under the academy's disciplinary procedure.

Contact Details

Information Commissioner's Office (ICO)

Tel: 0303 123 1113

Email: icocasework@ico.org.uk

Or via 'Live Chat' on www.ico.org.uk

Appendix A Definitions

(a)	Personal Information
	Information relating to a living individual who can be identified from that information or from other information in possession of the organisation. This is information that affects a person's privacy whether in their personal or family life, business or professional capacity and includes the name, address and telephone number of an individual. It will also include information on a person's medical history, an individual's salary details and includes expression of opinion about the individual and of the intentions of the organisation in respect of that individual. Personal information also includes CCTV images and photographs which enable the identification of an individual
(b)	Special Categories of Personal Information
	Is defined in the Act as racial or ethnic origin, political opinions, religious beliefs, trade union membership, physical or mental health, sex life, criminal convictions (see update November 2019 www.ico.org.uk)
(c)	Data Subject
	Any living individual who is the subject of personal information held by an organisation e.g. a learner, parent, member of school staff, council employee, agency worker, casual worker, customer, client, member of the public, partnership worker, councillor
(d)	Processing
	Any operation relating to information including: organising, retrieving, disclosing or otherwise making information available, deleting, obtaining, recording, altering, adding to, or merging
(e)	Third Party
	Any individual or organisation other than the information subject, the information controller or its employees or agents