



GLOBAL ACADEMY
MAKEUP • HAIR • PRODUCTIONS

INFORMATION HANDLING, RETENTION AND DISPOSAL & PRIVACY SECURITY POLICY

1. Introduction

Information is a vital asset to any organisation, and this is especially so in a knowledge-driven organisation such as Global, where information will relate to learning and teaching, research, administration and management. This policy is concerned with the management and security of Global information assets (an information asset is defined to be an item or body of information, an information storage system or an information processing system which is of value to Global) and the use made of these assets by its members and others who may legitimately process Global information on behalf of Global.

This overarching policy document provides an overview of information security and lists a hierarchical set of policy documents (sub-policies) which taken together constitute the Information Security Policy of Global.

2. Purpose

An effective Information Security Policy provides a sound basis for defining and regulating the management of information systems and other information assets. This is necessary to ensure that information is appropriately secured against the adverse effects of failures in confidentiality, integrity, availability and compliance which would otherwise occur.

3. Scope

The documents in the Information Security Policy set apply to all information assets which are owned by Global, used by Global for business purposes or which are connected to any networks managed by Global.

The documents in the Information Security Policy set apply to all information which Global processes, irrespective of ownership or form.

The documents in the Information Security Policy set apply to all members of Global and any others who may process information on behalf of Global.

4. Structure

The Information Security Policy document set is structured in accordance with the recommendations set out in the “UCISA Information Security Toolkit” which in turn, is based on the control guidelines set out in the industry standard ISO 27001.

This top-level document lists a set of other sub-policy documents which together constitute the Information Security Policy of Global. All these documents are of equal standing. Although this policy set should be internally consistent, for the removal of any doubt, if any inconsistency is found between this overarching policy and any of the sub-policies, this overarching policy will take precedence.

Each of the sub-policy documents only contains high-level descriptions of requirements and principles. They do not and are not intended to include detailed descriptions of policy implementation. Such details will, where necessary, be supplied in the form of separate procedural documents which will be referenced from the relevant, individual sub-policy documents.

5. Information security principles

Global has previously (in its original Information Access and Security Policy, 2002) adopted the following principles, which continue to underpin this policy:

1. Information will be protected in line with all relevant University policies and legislation, notably those relating to data protection, human rights and freedom of information.
2. Each information asset will have a nominated owner who will be assigned responsibility for defining the appropriate uses of the asset and ensuring that appropriate security measures are in place to protect the asset
3. Information will be made available solely to those who have a legitimate need for access.
4. All information will be classified according to an appropriate level of security.
5. The integrity of information will be maintained.
6. It is the responsibility of all individuals who have been granted access to information to handle it appropriately in accordance with its classification.
7. Information will be protected against unauthorised access.
8. Compliance with the Information Security policy will be enforced.
9. Governance

Responsibility for the production, maintenance and communication of this top-level policy document and all sub-policy documents lies with Global's CEO.

This top-level policy document has been approved by Global's CEO. Substantive changes may only be made with the further approval of the CEO.

Each of the documents constituting the Information Security Policy will be reviewed annually. It is the responsibility of the CEO to ensure that these reviews take place. It is also the responsibility of the CEO to ensure that the policy set is and remains internally consistent.

Changes or additions to the Information Security Policy may be proposed by any member of staff, via their Head of School or Division to the CEO.

Any substantive changes made to any of the documents in the set will be communicated to all relevant personnel.

6. Privacy policy details

This notice sets out how we collect, use and store your personal data.

When you interact with us by phone, mail, in person or online, we often receive personal information about you. We are registered with the Information Commissioner's Office as a data controller in respect of your personal data for the purposes of data protection law and are responsible for ensuring that we use your personal data in compliance with data protection law. Our ICO registration number is **ZA544713**

We are committed to protecting your privacy. We will always keep your personal information safe and will never sell it to third parties. We will be clear and open with you about why we collect your personal information and how we use it. Where you have choices, this notice explains them to you and we will respect your wishes.

7. How we collect information

We collect your personal data where we receive information about you directly, whether face-to-face, by phone, and by e-mail; when you enquire or apply for employment with us; or where we receive information about you from third parties, for example where you are being referred to one of our courses by a partner agency. However, third parties should only provide us with this information where you have given them permission to share your information and you should raise any concerns about this with your referring agency.

This information may include, but is not limited to, your name, address, contact telephone number, email address, and relevant necessary information for specific course such as national insurance number; substance use, employment status or offending status. Additionally, in running and maintaining our website we may collect and process the following data about you: Information about your use of our site including details of your visits such as pages viewed, length of visits and the resources that you access.

A 'Cookie' is a file in your web browser that enables us to recognise your computer when you visit globalmakeupacademy.com and make our site quicker and easier to use (e.g., login fields may be pre-filled with your details). Cookies are also essential to the functioning of certain parts of the site, and we use them to collect information about how the site is used, such as how many people visit and return and what products are being viewed.

We do not routinely collect any personal data about you through our Website, however, we may collect your personal data whenever you provide us with information through the website, for example when you:

- submit personal information to us using our online forms;
- enquire about our activities;
- register with us;
- undertake one or more of our online courses:

8. How we use your information

Your personal data may be stored and processed by Global Make up, Hair & Productions Academy Ltd in the following ways and for the following purposes:

- Providing you with the services, products or information you have requested or been referred for
- Managing our relationship with you
- Monitoring your individual progress and outcomes
- Undertaking anonymised statistical analysis (we won't be able to identify individuals from this data)
- Reporting to the appropriate legal and regulatory authorities, and complying with law;
- Understanding how we can improve our services, products or delivery.
- Processing your application for employment and monitoring our recruitment practice anonymously
- Managing your employment with us once recruited

We can use your personal data in these ways because either:

- you have consented to such use;
- we have a contract with you;
- we have legal and regulatory obligations that we must comply with;
- the use of your personal data is necessary for the legitimate business interests of our company
- we may need to establish, exercise or defend our legal rights or for the purpose of legal proceedings.

9. How long we keep your information

- We hold your personal information for as long as we have a legal or business reason to do so, which generally means for as long as you remain engaged with Global Make up Hair & Productions Academy for seven years as required by the National Open College Network where you have completed an accredited course; or as required to meet our legal obligations, including for 6 years following termination of employment as required by HMRC resolve disputes or enforce our agreements. We will always store it securely and will not use it for any other purpose to those listed above.
- Disposal of your personal information will be completed securely after the 7 years.

10. Disclosure of your information to Third Parties

We may need to share your information with third parties where you have been referred by a partner agency, including to confirm your attendance, completion and outcome feedback; or where we are required to disclose your identity for regulatory and legal purposes.

Your personal data is only accessed by employees of Global Make Up Academy or such companies (e.g. the National Open College Network) that have a need to process your data for the purposes described in this notice.

We may also share your personal data

- When you have requested referral or contact with third parties to help coordinate support for you and/or to signpost you to services provided by other organisations;
- If we sell all or part of the company, we may disclose your personal data to the buyer for legal or regulatory and continuity purposes
- To third party agents, contractors, professional or legal advisors for the purposes of providing services to us. These third parties will be subject to confidentiality requirements, and they will only use your personal data as described in this privacy notice
- Where required by law, to the police, regulatory bodies or legal advisors, for example if we are under a duty to disclose your personal data in order to comply with any legal obligation, establish, exercise or defend our legal rights.
- To secure references and 'disclosure' from the Disclosure and Barring Service relating to your employment but will seek your consent prior to doing so.

11. Your Rights

You have a number of legal rights in relation to the personal data that we hold about you. These rights include:

- the right to obtain information regarding the processing of your personal data and access to the personal data which we hold about you;
- the right to withdraw your consent to our processing of your personal data at any time. However, we may still be entitled to process your personal data if we have another legitimate reason (other than consent) for doing so.
- in some circumstances, the right to receive some personal data in a structured, commonly used and machine-readable format and/or request that we transmit that data to a third party where this is technically feasible. Please note that this right only applies to personal data which you have provided to us;

- the right to request that we rectify your personal data if it is inaccurate or incomplete;
- the right to request that we erase your personal data in certain circumstances. Please note that there may be circumstances where you ask us to erase your personal data but we are legally entitled to retain it;
- the right to request that we restrict our processing of your personal data in certain circumstances. Again, there may be circumstances where you ask us to restrict our processing of your personal data but we are legally entitled to refuse that request; and,
- the right to lodge a complaint with the data protection regulator (details of which are provided below) if you think that any of your rights have been infringed by us.

You can exercise your rights by contacting us at the address at the end of this notice.

You can find out more information about your rights by contacting the Information Commissioners Office, or by searching their website at <https://ico.org.uk/>.

12. Social Media

By using our social media sites and pages, including Facebook and Twitter, you consent to our collection and use of the information you provide in the way set out in this policy.

If you do not agree to this policy please do not use our sites, social media pages or services.

13. How we store keep your information safe and dispose of your information

Global Make up Hair and Productions Academies Ltd hold and stores all information on secure databases and servers entirely within the United Kingdom that are protected through extensive electronic, physical and managerial measures to ensure your information is kept safe and secure.

Where we use third parties suppliers involving the processing of data, these are subject to detailed confidentiality agreements and contracts relating to any personal data they have access to.

When we change our processes and procedures we consider the need to undertake a Data Protection Impact Assessment to ensure we are clear of any impact on data protection of proposed changes.

We respect the fact that your personal information is your information, and we'll make it easy for you to update or change your personal details or consents. Please help us to help you by letting us know if your contact details change or if you spot any errors in the information we hold about you by contacting us at the address below.

14. Exams results

Exams and students portfolios, and all educational data relating to their course of study need to be archived for up to 4 years after completion – if the student does not collect their portfolio after being contacted they will be securely shredded Using confidential shredders.

15. Home and Mobile working Security of Data

All data must be processed, managed and stored in line with the General Data Protection Regulations (GDPR).

Employees must ensure that all information stored and accessed (including written information and that held on computer) is secure and cannot be accessed by other parties. Please see Data Protection and Security Policy. Failure to keep information secure will be considered a serious matter and dealt with under the Disciplinary Policy and Procedure.

16. Contacting us

The FUSE Redeeming Our Communities

Warburton Lane

Partington

M314BU

Email: leilam@globalmakeupacademy.co.uk

Website: www.globalmakeupacademy.co.uk

Reviewed by	Compliance & Quality Assurance Administrator
Reviewed	Annually, before start of a new academic year
Last Review	03/06/2025
Review Date	30/08/2026

Reviewed: Signed: B Levy..... **Date:** 03/06/25

Benjamin Levy
Compliance & Quality Assurance Administrator