



Data Protection (Including GDPR Compliance) Policy

Approved by: Lisa Robertson

Last reviewed on: 03/2026

Next review due: 03/2027

introduction

At New You Hair Academy, we highly value your privacy and are dedicated to adhering to the General Data Protection Regulations (GDPR). Our commitment is to keep you well-informed about the data we collect, its utilisation, the entities we share it with, and the duration of its retention. This privacy notice, also referred to as a fair processing notice, has been designed to offer you clear and thorough information. Should you have any queries or concerns regarding your data, please feel free to reach out to our academy office.

Data Controller

New You Hair Academy Ltd is the Data Controller for the purposes of UK GDPR. This means the academy determines the purposes for which, and the manner in which, personal data is processed.

The designated Data Protection Lead is:

Lisa Robertson

Head of Teaching & Learning

Email: Lisa@NYHA.co.uk

New You Hair Academy Ltd is registered with the Information Commissioner's Office (ICO).

Categories of student & parent information that we collect, hold and share

At New You Hair Academy, we collect, store, and share various categories of student and parent information to ensure the smooth functioning of our educational services. Upholding the confidentiality and security of this data is our top priority. The following outlines the types of information we may collect, though this list is not exhaustive:

Personal Information:

This encompasses student and parent details such as names, unique student numbers, addresses, and parents' national insurance numbers.

Characteristics:

Information related to ethnicity, language, nationality, religion, country of birth, eligibility for Early Years student Premium, and free school meals.

Assessment and Academic Records:

Internal assessment results, externally set tests, student records, and curricular information.

Attendance Data:

Recording of attendance information, including sessions attended, number of absences, and reasons for absence.

Assessment Information:

Data scores, tracking information, and results from internal and external testing.

Safeguarding:

Information regarding safeguarding, such as relevant incidents or concerns.

Fixed-Term Suspension:

Details regarding any fixed-term suspensions.

Medical Information:

Including medical conditions, both physical and mental health-related, and any support received, including care packages and support providers.

Media:

Capture of photographs and videos for learning purposes, internal safeguarding and security, newsletters, and promotional materials.

Relevant Medical Information:

NHS data, health checks, physical and mental health care information, immunisation programs, and allergy information.

Special Educational Needs:

Details related to special educational needs, such as Education, Health, and Care Plans (EHCPs), statements, applications for support, and care plans.

School Meals:

The number of school meals taken by students.

Behavioural Information:

Records of student behaviour and related incidents.

CCTV Images and Audio:

Images and audio captured by CCTV cameras on our premises for security and monitoring purposes.

Court Orders or Prosecutions/Convictions:

Information regarding any court orders, prosecutions, or convictions.

Internet and Mobile Device Usage:

Monitoring of students' use of the internet and mobile electronic devices (e.g., iPads, Chromebooks) to ensure their safety, well-being, and responsible behaviour.

Additionally, we may receive data about students from other organisations, including other schools, local authorities, and the Department for Education, to support educational and administrative processes.

Why we collect and use this information

The collection and use of this information serve various purposes:

Support Student Learning:

Utilising data to tailor educational programs, instructional strategies, and support services based on individual needs and learning styles.

Monitor and Report on Student Progress:

Tracking and assessing students' academic development, identifying areas for improvement, and providing timely feedback and progress reports.

Provide Appropriate Pastoral Care:

Offering targeted pastoral support, guidance, and counselling based on students' personal and social circumstances.

Protect Student Welfare:

Prioritising the safety and welfare of students by implementing appropriate safeguarding measures and responding promptly to concerns or incidents.

Safeguard Students:

Identifying patterns, trends, and potential risks affecting students' safety and well-being, enabling the implementation of preventive measures and intervention strategies.

Assess the Quality of Our Services:

Evaluating the effectiveness and impact of educational provision through data analysis to identify areas of improvement and ensure the highest standard of education and support.

Administer Admissions Waiting Lists:

Managing admissions waiting lists fairly and transparently to ensure equitable access to our alternative provision.

Carry Out Research:

Utilising anonymized data for research purposes, with appropriate safeguards and permissions, to gain insights into educational practices, outcomes, and intervention effectiveness.

Comply with Data Protection Laws:

Adhering to legal requirements and regulations governing the sharing and processing of personal data, including GDPR and other relevant legislation.

Promote the Objects and Interests of the Alternative Provision:

Assisting in making informed decisions, developing targeted initiatives, and effectively engaging with stakeholders.

We handle all personal data with utmost care, ensuring strict confidentiality, security, and compliance with data protection regulations.

The lawfulness of processing

In compliance with GDPR and other relevant legislation, New You Hair Academy ensures that the collection and processing of student information are conducted lawfully. The lawfulness of processing is determined by the conditions set forth in Article 6 of GDPR. These conditions include:

Consent:

Processing of student information is lawful if the data subject (student or legal guardian) has given explicit consent for one or more specific purposes.

Legal Obligations:

Processing is necessary to comply with the legal obligations of the data controller (New You Hair Academy).

Vital Interests:

Processing is necessary to protect the vital interests of the student, such as their health and safety.

Public Interest:

Processing is necessary for tasks carried out in the public interest or in the exercise of official authority vested in the data controller, specifically related to the provision of education.

The lawful basis for collecting and processing student information, including sensitive or special information, is further defined under Article 9 of GDPR. The conditions justifying the lawful processing of such information are:

Explicit Consent:

Processing is lawful if the data subject has given explicit consent for the specific purposes outlined.

Obligations of the Controller or Data Subject:

Processing is necessary to fulfil the obligations of the data controller or the data subject.

Vital Interests:

Processing is necessary to protect the vital interests of the data subject, such as their health and well-being.

Not-for-Profit Organisations:

Processing is carried out by a foundation or not-for-profit organisation, including religious, political, philosophical organisations, and trade unions.

Public Interest/Public Health: Processing is necessary for reasons of public interest in the area of public health.

Collecting student information

At New You Hair Academy, we understand the importance of collecting student information transparently and responsibly. When gathering personal information, we provide clear communication to inform you about the necessity of providing certain student information. We indicate whether there is a legal requirement to provide such information or if you have the option to choose whether to provide it.

In cases where there is no legal obligation to provide the information, we clearly explain why we need it and the potential consequences if it is not provided. Our aim is to ensure that you have a comprehensive understanding of the reasons behind the collection of student information, empowering you to make informed decisions.

Data Retention:

Personal data will only be retained for as long as necessary to fulfil the purposes for which it was collected, including satisfying legal, accounting or reporting requirements. Retention periods are determined in accordance with statutory guidance and the academy's Records Retention Schedule.

Safeguarding records are retained in line with national safeguarding guidance.

Your Rights Under UK GDPR:

Under UK GDPR, individuals have the right to:

- Access their personal data (Subject Access Request)
- Rectification of inaccurate data
- Erasure ("right to be forgotten") where applicable
- Restrict processing
- Object to processing in certain circumstances
- Data portability (where applicable)

Requests can be made in writing or by email to the Data Protection Lead. We will respond within one calendar month in accordance with UK GDPR.

Data Security:

The academy implements appropriate technical and organisational measures to protect personal data, including:

- Secure cloud-based systems with restricted access
- Password protection and multi-factor authentication where appropriate
- Secure storage of paper records
- Role-based access to safeguarding information
- Staff training in data protection responsibilities

Data Breach Response:

At New You Hair Academy, we understand the critical importance of safeguarding the personal data of our students and parents. Despite our stringent security measures, there is always a potential risk of a data breach. A data breach refers to any unauthorised access, disclosure, alteration, or destruction of personal data.

In the event of a data breach, we are committed to taking immediate action to mitigate any potential harm and to comply with our obligations under the General Data Protection Regulation (GDPR). Our response to a data breach will follow a predefined protocol aimed at minimising the impact on affected individuals and ensuring transparency in our communication.

Steps We Will Take in the Event of a Data Breach:**1. Identification and Assessment:**

Our first priority will be to promptly identify and assess the nature and scope of the data breach. This involves determining what data has been compromised, how it occurred, and the potential consequences for individuals affected.

2. Containment and Remediation:

Once the breach has been identified, we will take immediate steps to contain the breach and prevent any further unauthorised access or disclosure of personal data. This may involve temporarily suspending affected systems or services and implementing additional security measures.

3. Notification:

If the breach is likely to result in a risk to the rights and freedoms of individuals, we will notify the Information Commissioner's Office (ICO) within 72 hours of becoming aware of it, where required under UK GDPR. We will also notify affected individuals promptly, providing clear and transparent information about the nature of the breach, the potential risks involved, and any steps they can take to protect themselves.

4. Investigation and Review:

Following the initial response, we will conduct a thorough investigation into the causes of the data breach and identify any weaknesses or vulnerabilities in our systems or procedures that may have contributed to the incident. Based on our findings, we will take appropriate corrective actions to prevent similar breaches from occurring in the future.

5. Documentation and Reporting:

Throughout the process, we will maintain detailed records of the data breach, including the actions taken and any communications issued. We will also report the breach to the relevant authorities as required by law and cooperate fully with any investigations or inquiries.

Contact Information:

If you have any concerns or questions regarding data protection or wish to report a potential data breach, please contact us immediately at:

Email: Lisa@NYHA.co.uk

International Transfers

The academy does not routinely transfer personal data outside the UK. Where cloud-based systems are used, we ensure that appropriate safeguards are in place in line with UK GDPR.

Complaints

We value your feedback and take any complaints regarding the collection and use of personal information seriously. If you believe that our practices are unfair, misleading, inappropriate, or if you have any other concerns regarding our data processing, we encourage you to bring them to our attention in the first instance.

If you prefer to escalate your complaint further, you have the right to contact the Information Commissioner's Office (ICO). The ICO is an independent authority that oversees data protection in the United Kingdom.

You can report your concern online by visiting their website at <https://ico.org.uk/concerns/>.

If you prefer to speak with someone directly, you can reach the ICO by calling 0303 123 1113. Additionally, you have the option to send a written complaint to the following address:

Information Commissioner's Office

Wycliffe House, Water Lane, Wilmslow, Cheshire, SK9 5AF

We encourage open communication and are committed to addressing any concerns raised by our stakeholders. Your feedback is important to us, and we will take appropriate measures to investigate and resolve any complaints regarding our data processing practices.