School of Coding & AI

//: Building_better_futures_through_code

## HIGHER EDUCATION

# Data Protection Policy

**Policy Owner: Mandeep Athwal**

| Full Name | Position | Signature | Date | Review Cycle |
|---|---|---|---|---|
| Mandeep Athwal | CEO |  | 01.09.2025 | Annual |

School of Coding Higher Education collects and uses personal information about Students, Applicants, staff, Alumni, Partners, and other stakeholders who come into contact with the institution. This information is gathered in order to enable it to provide education and other associated functions. In addition, there may be a legal requirement to collect and use the information to ensure that the institution complies with its statutory obligations.

Institutions have a duty to be registered, as Data Controllers, with the Information Commissioner's Office (ICO) detailing the information held and its use. These details are then available on the ICO's website. Institutions also have a duty to issue a Privacy Notice to all Students and staff, which summarises the information held about individuals, the reason it is held, and the parties with whom it may be shared.

School of Coding Higher Education has appointed Harry Athwal as its Data Protection Officer (DPO), responsible for monitoring compliance with data protection laws and serving as the point of contact for data subjects and the Information Commissioner's Office (ICO)

School of Coding Higher Education is also committed to ensuring that its staff are aware of data protection policies, legal requirements, and receive adequate training. All staff receive training on data protection principles and responsibilities as part of their induction, and regular refresher training is provided. School of Coding Higher Education maintains records of training completion. Compliance with this policy is mandatory for all staff employed by the institution and any third party contracted to provide services within the institution.

**Purpose**

This policy is intended to ensure that personal information is dealt with correctly and securely and in accordance with the Data Protection Act 2018, UK General Data Protection Regulations (UK GDPR), and other relevant legislation. It applies to information regardless of how it is collected, used, recorded, stored, and destroyed, irrespective of whether it is held in paper files or electronically.

All staff involved with the collection, processing, and disclosure of personal data will be aware of their duties and responsibilities by adhering to this policy. This Data Protection Policy also reflects the expectations of the Office for Students (OfS) regulatory framework, ensuring that all processing of personal data supports the institution's obligations under OfS Conditions of Registration, particularly in providing accurate, transparent information to students and stakeholders.

**What is Personal Information?**
Personal information (personal data) is defined as any information relating to a living individual who can be identified, directly or indirectly, from that information or from other data in the institution's possession.

**Data Protection Principles**
School of Coding Higher Education will collect and process personal data in compliance with the data protection principles under Article 5 of the UK GDPR. This means personal data shall be:

• **Processed lawfully, fairly, and in a transparent manner –** individuals will be informed about what is being collected, why it is being collected, and how it will be used, with whom it will be shared. We do this through the institution's privacy notice.
• **Collected for specific, explicit, and legitimate purposes –** data will be collected for a defined and legitimate purpose only.
• **Adequate, relevant and limited –** we will only collect what is needed and nothing more
• **Accurate and kept up-to-date –** reasonable steps will be taken to maintain an accurate record.
• **Storage Limitation –** we will only keep data for as long as is necessary and in accordance with relevant legislation. Personal data will be retained only as long as necessary to fulfil the purposes for which it was collected, in line with the School of Coding Higher Education's Data Retention Schedule. A summary of retention periods for key records (e.g. student records, finance, HR) is available on request
• **Security of information processed** – the institution will protect against unauthorised or unlawful processing and against accidental loss, destruction or damage.

School of Coding Higher Education processes personal data under the following lawful bases as defined by the UK GDPR:

- Where processing is necessary for the performance of a contract with the data subject (e.g. providing education services);
- Where processing is necessary to comply with a legal obligation (e.g. regulatory reporting);
- Where processing is necessary for tasks carried out in the public interest (e.g. educational functions);
- Where processing is necessary for the legitimate interests of the institution or a third party, except where such interests are overridden by the rights of the data subject;
- Where the individual has given clear, informed consent.

**Individual Rights**
School of Coding Higher Education also recognises the rights of individuals in respect of the information the institution holds about them. Any requests to recognise these rights will be fully considered and evaluated so that the individual can be informed whether they can/cannot exercise the rights under their particular circumstances. These rights are:

- **Right to be Informed** – about how their data is being used
- **Right of Access –** to be able to access their data
- **Right to Rectification –** right to correct information about them that is incorrect
- **Right to Erase –** to have their data erased when they no longer want it to be used
- **Right to Restrict Processing** – to restrict how their data is used
- **Right to Data Portability** – to move their data from one organisation to another
- **Right to Object –** to object to their data being used at all
- **Right to Automated Decision making, including Profiling** – decision-making (where there is no human involvement) and profiling are restricted under the GDPR.

The restriction can be lifted under three circumstances;
1) For a contractual basis;
2) For a legal basis;
3) Based on an individual's explicit consent.

**Privacy Notice**
School of Coding Higher Education shall be transparent about the intended processing of data and communicate these intentions via privacy notice to staff and Students prior to the processing of an individual's data. Notifications shall be in accordance with ICO guidance and, where relevant, be written in an understandable form.

There may be circumstances where School of Coding Higher Education is required either by law or in the best interests of our students or staff to pass information to external authorities, for example:

- Office for Students (Ofs)
- Higher Education Statistics Agency(HESA)
- Local authorities
- Ofsted
- Department of health and social care

These authorities are up to date with data protection laws and have their own policies relating to the protection of any data that they receive or collect.

The intention to share data relating to individuals with an organisation outside of our institution shall be clearly defined within privacy notices, and details of the basis for sharing shall be given. Data will be shared with external parties in circumstances where it is a legal requirement to provide such information.

Any proposed change to the processing of an individual's data shall first be notified to them. Under no circumstances will the institution disclose information or data.

**Data Security**

In order to assure the protection of all data being processed and make informed decisions on processing activities, we shall undertake an assessment of the associated risks of proposed processing and equally the impact on an individual's privacy in holding data related to them. Risk and impact assessments shall be conducted in accordance with the guidance given by the ICO. Where new processing activities present a high risk to individuals' rights and freedoms, the School of Coding Higher Education will conduct Data Protection Impact Assessments (DPIAs) in line with ICO guidance. Security of data shall be achieved through the implementation of proportionate physical and technical measures. Nominated staff shall be responsible for the effectiveness of the controls implemented and reporting of their performance. The security arrangements of any organisation with which data is shared shall also be considered, and where required, these organisations shall provide evidence of their competence in the security of shared data.

**Subject Access Requests**

Individuals have a legal right to request access to personal data held about them. Request should:

- Should be in writing and be legible in order to correctly identify the requester.
- Must be specific with regard to records or data being requested in order to avoid excessive requests
- Must follow the process of confirming identification
- Although we accept requests that can be given verbally or via other mediums, we will request that you please use and complete our form from the website to support this process and comply with the need to identify the requester and the data being requested.

**Confirming Identity**

The institution will take reasonable steps to confirm the identity of the requester. However, the institution will not make this identification process unnecessarily onerous and in cases where the requester is already known to the institution (e.g. an existing member of staff, a known parent), formal identification will not be sought.

**Timing of Requests**
All requests will be responded to as promptly as possible, and in any event, a response must be provided by no later than 1 month from the day of receipt; however, the 1-month time limit will not commence until clarification of information and or identification is sought. Where the case is considered to be complex, the deadline can be extended to 60 days. The requester should be kept informed of any delays.

**Access to Personal Data by an Authorised/ Legal Agent**
When an agent makes a request on behalf of a Data Subject, signed authorisation from the Data Subject will be required. The institution may still check directly with the Data Subject whether he or she is happy with the agent receiving the personal data, and should highlight the implications of the request.

Any request received from an agent must be accompanied by a signed Form of Authority [permission] from the Data Subject. No proof of identity for a Data Subject is required when the application comes from a professionally recognised agent such as a Solicitor.

**Information Containing Third-Party Data**
The institution may refuse a subject access request where releasing that information would also involve disclosing information about another individual, except in cases where:

- That individual has consented to disclosure; or
- It is reasonable in all circumstances to comply with the request without that individual's consent.

The institution will seek to balance the rights of the requester with the rights of the third party and only release information if, in all circumstances, it is reasonable to do so.

**Refusing a Request**
School of Coding Higher Education uses the presumption of release as the starting point for all valid subject access requests. Where there is a legitimate reason why information should not be disclosed (e.g. the prevention or detection of crime, legal privilege, National Security considerations) the applicant will be informed of the reasons why (except in circumstances where disclosure may prejudice the purpose of the exemption applied) and of their right to appeal.

**Amendments to Inaccurate Records**
School of Coding Higher Education acknowledges individuals' right to challenge the accuracy of the personal data held about them where they believe it to be inaccurate or misleading. Where information is found to be factually inaccurate, it will be updated immediately. Where there is a dispute between the institution and the data subject as to the accuracy of information, a note will be made on the record to that effect, and both sets of information will be kept on the file.

**Objections to Processing**
Individuals have the right to request that the processing of information about them be restricted or ceased if they believe the information to be inaccurate or being held unnecessarily. School of Coding Higher Education must investigate any such request and rectify if necessary. The Data Subject should be informed before any restriction is lifted.

**Releasing personal information to prevent or detect crime**
It is the institution's policy to cooperate wherever possible with requests for personal information for the prevention or detection of crime or identification or apprehension of suspects, but only after satisfactory checks have been completed to protect the rights of Data Subjects. Information will only be released where disclosure meets the criteria outlined in the UK GDPR
Requests will only be considered from an agency with a crime or law enforcement function, including the Police, HMRC, the UK Border Agency, or the Benefit Fraud sections of DWP or other Local Authorities.

Requests must be in writing and be clear on what is being asked for and why the release of the information is critical to the investigation.

Only information directly relevant to the purpose stated will be released, and only the minimal possible to enable the law enforcement agency to do their job. The transfer of information will be via a secure channel (e.g. secure email or special delivery post).

**Sharing Personal Data with Third Parties**
Personal data about Students will not be disclosed to third parties without the consent of the students unless it is required by law or in the best interest of the Students. Data may be disclosed to the following third parties without consent:

**• Other institutes**

If a student transfers from School of Coding Higher Education to another institution, their academic records and other data that relate to their health and welfare will be forwarded to the new institution.

**• Examination authorities**
This may be for registration purposes, to allow the students at School of Coding Higher Education to sit examinations set by external exam bodies.

**• Health authorities**
As obliged under health legislation, School of Coding Higher Education may pass on information regarding the health of students in the institution to monitor and avoid the spread of contagious diseases in the interest of public health.

**• Police and courts**
If a situation arises where a criminal investigation is being carried out, we may have to forward information to the police to aid their investigation. We will pass the information on to the courts as and when it is ordered.

**• Social workers and support agencies**
In order to protect or maintain the welfare of our students, it may be necessary to pass personal data on to social workers or support agencies.

**• Educational division**

School of Coding Higher Education may be required to pass data on in order to help the government monitor the national educational system and enforce laws relating to education.

Subject access requests should be made in writing to: CEO Mandeep Athwal, The School of Coding & AI, Pendeford Business Park, Wolverhampton, WV9 5HB.

**Photographs and Video**
Images of staff and students may be captured at appropriate times and as part of educational activities for use in the institution only.
Unless prior consent from students/staff has been given, the institution shall not utilise such images for publication or communication to external sources.

It is the institution's policy that external parties may not capture images of staff or students during such activities without prior consent. Where the image of another individual is captured in the photo, it is prohibited for individuals to make these public or post on social media.

**Data Disposal**
The institution recognises that the secure disposal of redundant data is an integral element to compliance with legal requirements and an area of increased risk. All data held in any form of media (paper, tape, electronic) shall only be passed to a disposal partner with demonstrable competence in providing secure disposal services. All data shall be destroyed or eradicated to agreed levels meeting recognised national standards, with confirmation at the completion of the disposal process. Disposal of IT assets holding data shall be in compliance with ICO guidance.

**Complaints**
Complaints regarding this policy should be addressed to the Chairperson of the Governing Body, who will determine whether they fall under the institution's complaints procedure. Complaints outside the scope of the internal process can be referred to the institution's Data Protection Officer or directly to the ICO.

**Review**
This policy will be reviewed as it is deemed appropriate, but no less frequently than every 2 years. The policy review will be undertaken by the CEO or a nominated representative.

**Approved by: Manny Athwal**
**Date: September 2025**