# Data Protection, Privacy, Storage and Retention Guidance

**In Education- Version 4**

| | |
|---|---|
| Directorate: | Communities and Neighbourhoods- Employment and Training Services |
| Validated by: | Tanzeem Ahmed |

This guidance will be reviewed on an annual basis. Poplar HARCA reserves the right to amend this guidance, following consultation, where appropriate.

| | |
|---|---|
| Date created: | November 2023 |
| Date of next review: | November 2024 |

## 1. What is this guidance about?

At Poplar HARCA we're committed to protecting and respecting your privacy. This guidance explains when and why we collect personal information about people, how we use it, the conditions under which we may disclose it to others and how we keep it secure.

*Roles and responsibilities*

1 The ultimate responsibility for the Poplar HARCA's compliance with Data Protection Legislation lies with the Chief Executive Officer (CEO).

2 The Senior Leadership Team is responsible for maintaining this procedure and may delegate responsibility for approving changes to the guidance to committees or individual members of staff.

3 The Assistant Director of Business Support Services / DPO Officer has overall operational responsibility for compliance with data protection law, and advising the business (or arranging advice for the business) on data protection law.

4 The Assistant Director of ICT is responsible for ensuring that appropriate technical measures are in place to secure and ensure the availability of electronic information, including Personal Data.

Managers within every business area are responsible for implementing and ensuring compliance with data protection procedures in their areas. This includes the requirement to take all reasonable steps to ensure compliance by third parties which process Personal Data for which Poplar HARCA is the Data Controller.

## 2. Who is this guidance for?

This guidance is for all staff, volunteers, learners, employers, other stakeholders and third-party provisions and partnerships to ensure awareness of Poplar HARCA commitment to data protection.

## 3. How do we collect information from you?

We obtain information about you when you or a partner agency contact us to express an interest in a training programme and/or enrol on one of our training programmes and via application forms when applying for vacancies.

## 4. What type of information is collected from you?

The personal information we collect includes your name, address, email address, telephone number, information regarding eligibility for funding (including NI number), residency status and information regarding other courses you have undertaken. This list is not exhaustive and we may require additional information for enrolments and job applications such as emergency contact details, employment history, copies of identification and information relating to health and disabilities. We may also collect information relating to employers, such as address, email address, telephone number, sector, and number of employees.

## 5. How is your information used?

We may use your information to:

- process a claim for funding relating to your chosen course through our contractors
- to carry out our obligations arising from any contracts entered into by you and us
- seek your views or comments on the services we provide

- notify you of changes to our services
- send you communications which you have requested and that may be of interest to you
- To match individual skills and experience to suitable advertised roles, where necessary

## 6. Our commitment

*Poplar HARCA will:*

- Process Personal Data in accordance with the instructions from its Contractors
- Process the Personal Data only to the extent and in such a manner as is necessary for the provision of the services or as is required by Law or any Regulatory Body
- Implement appropriate technical and organisational measures to protect the Personal Data against unauthorised or unlawful processing and against accidental loss, destruction, damage, alteration or disclosure. These measures shall be appropriate to the harm which might result from any unauthorised or unlawful processing, accidental loss, destruction or damage to the Personal Data and having regard to the nature of the Personal Data which is to be protected
- Take reasonable steps to ensure the reliability of any Contractor Personnel who have access to the Personal Data
- Obtain prior written consent from Contractors in order to transfer the Personal Data to any sub-contractor or other third parties for the provision of the Services
- Not publish, disclose or divulge any of the Personal Data to any third party unless directed in writing to do so by the Contractor
- Notify Contractor within 5 working days if it receives a request from a Data Subject to have access to that person's Personal Data; or a complaint or request relating to obligations under the General Data Protection Regulations
- Provide Contractor with full co-operation and assistance in relation to any complaint or request made, including by providing Contractor with full details of the complaint or request; complying with a data access request within the relevant timescales set out in the General Data Protection Regulations and in accordance with ESFA/GLA's instructions
- Provide Contractor with any Personal Data it holds in relation to a Data Subject (within the timescales required by the Contractor)
- Provide Contractor with any information requested by them or their representatives
- Permit Contractor or Contractor representative (subject to reasonable and appropriate confidentiality undertakings), to inspect and audit Poplar HARCA Data Processing activities (and/or those of its agents, subsidiaries, and sub-contractors) and comply with all reasonable requests or directions by Contractor to enable the Contractor to verify and/ or procure that Poplar HARCA is in full compliance with its obligations under all contracts
- Provide a written description of the technical and organisational methods employed by Poplar HARCA for processing Personal Data (within the timescales required by ESFA/GLA) and not Process Personal Data outside the European Economic Area without the prior written consent of Contractor and, where Contractor consents to a transfer, to comply with: the obligations of a Data Controller under the General Data Protection regulations by providing an adequate level of protection to any Personal Data that is transferred
- If Poplar HARCA provide services to learners claiming out of work benefits, the Secretary of State for Work and Pensions (or their successor) is the Data Controller in relation to Personal Data which Poplar HARCA is required to provide to the Secretary of State for Work and Pensions under any enactment. This Clause 16 will be enforceable by the Secretary of State for Work and Pensions in relation to any Personal Data processed by Poplar HARCA on their behalf

*Who has access to your information?*

Poplar HARCA will supply to the Contractor**,** data on each individual learner, in accordance with the data collections framework set out in the '*Individualised Learner Record (ILR) specification*
Poplar HARCA will supply the Contractor with data in accordance with the following:

- in line with agreed audit arrangements
- in adherence with General Data Protection Regulations

- to support payments to be made
- to enable reconciliation to take place
- to support the contract management and allocation processes

All information is held on secure password protected systems and secure filing cabinets. We will not sell or rent your information to third parties. We will not share your information with third parties for marketing purposes.

## 7. Your rights

Under Data Protection legislation 2018, you have various rights with respect to our use of your personal data:

*Right to Access*- you have the right to request a copy of the personal data that we hold about you by contacting us at the email or postal address given above. Please include with your request information that will enable us to verify your identity. We will respond within 1 month of request. Please note that there are exceptions to this right. We may be unable to make all information available to you if, for example, making the information available to you would reveal personal data about another person, if we are legally prevented from disclosing such information, or if there is no basis for your request, or if it is excessive.
*Right to rectification*- we aim to keep your personal data accurate and complete. We encourage you to contact us using the contact details provided above to let us know if any of your personal data is not accurate or changes, so that we can keep your personal data up-to-date.

*Right to erasure*- you have the right to request the deletion of your personal data where, for example, the personal data are no longer necessary for the purposes for which they were collected, where you withdraw your consent to processing, where there is no overriding legitimate interest for us to continue to process your personal data, or your personal data has been unlawfully processed. If you would like to request that your personal data is erased, please contact us using the contact details provided above.

*Right to object*-in certain circumstances, you have the right to object to the processing of your personal data where, for example, your personal data is being processed on the basis of legitimate interests and there is no overriding legitimate interest for us to continue to process your personal data, or if your data is being processed for direct marketing purposes. If you would like to object to the processing of your personal data, please contact us using the contact details provided above.

*Right to restrict processing*- in certain circumstances, you have the right to request that we restrict the further processing of your personal data. This right arises where, for example, you have queried the accuracy of the personal data we hold about you and we are verifying the information, you have objected to processing based on legitimate interests and we are considering whether there are any overriding legitimate interests, or the processing is unlawful and you elect that processing is restricted rather than deleted. Please contact us using the contact details provided above.

*Right to data portability*- in certain circumstances, you have the right to request that some of your personal data is provided to you, or to another data controller, in a commonly used, machine-readable format. This right arises where you have provided your personal data to us, the processing is based on consent or the performance of a contract, and processing is carried out by automated means. If you would like to make such a request, please contact us.

*18 or Under*

We are committed to safeguarding our learners which includes protecting the privacy of children aged under 18. For those aged under 18 parent/guardian's parental consent is gained where appropriate.

Every member of staff or volunteer has a responsibility for ensuring that learners are safeguarded while they are using Poplar HARCA services. Poplar HARCA organisational safeguarding standards recognises that we safeguard in a wide range of contexts with a diverse group of learners. Therefore, managing the risk to learners in these contexts can require different sets of knowledge and skills, and different responses, some of which are driven by statute and legislation. Our safeguarding standards and behaviours seek to underpin

safeguarding in all of our practice and are derived from section 11 of the Children Act (2004) and the Care Act (2014) as well as best practice guidance such as "Working Together to Safeguarding Children 2018", KCSiE https://www.gov.uk/government/publications/keeping-children-safe-in-education--2
Our approach to safeguarding is measured against our company organisational standards.

*Please see additional safeguarding information within our Safeguarding Guidance.*

*Poplar HARCA Employees Rights*

*Right to be forgotten*- you can request your information and documentation to be erased from Poplar HARCA human resources records system. This request will only be accepted when an individual is resigning, retiring or has been subject to dismissal. You have a right to be forgotten which can be requested from *Candidates' right to request their info*- full export of all your data from our system can be requested. All data held on our system will be sent across within the 30-day time period. You have a right to request your information.

*Candidates' right to edit & update their information*- all employees have a right to edit and update their information.

*Consent to hold data*-all employees provide consent to hold their data in induction upon signing the 'Employee Data Form'.

*Data security compliance*- we are a UK company and our servers are based within the EU.

*Data security*- we use encryption to protect your data. All employees are informed at induction how their data will be processed.

## 8. Document Retention

We review our retention periods for personal information on a regular basis. We are legally required to hold some types of information to fulfil our statutory obligations including ESFA funding streams.

Internal staff files are archived 6 months after the leave date and retained for 3 years but you can request 'to be forgotten' prior to 6 months when your information, upon request can be securely deleted.

If either now or in the future the safe retention of information is at risk, i.e. an organisation is closing down, the support services contracts and compliance manager will immediately contact the ESFA/GLA to discuss alternative arrangements.

For external documents e.g. qualification standards, generally from awarding organisations, these will be held by appropriate staff involved with the delivery of the programmes.

## 9. Document Disposal

Confidential information will be shredded by a professional company on regular basis in line with contractual requirements.
Confidential archived information will be shredded by a professional company, at the appropriate time – after the required duration of archiving has been carried out.

## 10. Data Breach

*Breach detection measures*

The following measures have been put into practice to assist in detecting and preventing a personal data breach:

- Appointment of a Data Protection Officer
- Heighted and improved security software, encryptions and threat detection

- Contracted professional business IT support company
- Clear reporting lines
- Staff training and awareness

The Assistant Director of Business Support Services / DPO Officer has overall operational responsibility for compliance with data protection law.

*Suspected breach investigation*

In the event that we are made aware of a breach, or a potential breach, an investigation will be carried out And the CEO will make a decision over whether the breach is required to be notified to the Information Commissioner's Office (ICO). A decision will also be made over whether the breach is such that the individual(s) must also be notified.
All suspected breaches will be logged on the Data Breach Log.

*Breach notification – ICO*

In accordance with the GDPR, we will notify the ICO of a breach which is likely to pose a risk to people's rights and freedoms. A risk to people's freedoms can include physical, material or non-material damage such as discrimination, identity theft or fraud, financial loss and damage to reputation.
Notification to the ICO will be done without undue delay and at the latest within **72 hours** of discovery. If we are unable to report in full within this timescale, we will make an initial report to the ICO, and then provide a full report in more than one instalment if so required.

The following information will be provided when a breach is notified:

- A description of the nature of the personal data breach including, where possible
- The categories and approximate number of individuals concerned
- The categories and approximate number of personal data records concerned
- The name and contact details of our Data Protection Officer, where more information can be obtained
- A description of the likely consequences of the personal data breach
- A description of the measures taken, or proposed to be taken, to deal with the personal data breach, including, where appropriate, the measures taken to mitigate any possible adverse effects

*Breach notification – individual*

In accordance with the GDPR, The Data Protection Officer will notify the individual whose data is the subject of a breach if there is a high risk to people's rights and freedoms.
A high risk may be, for example, where there is an immediate threat of identity theft, or if special categories of data are disclosed online.
This notification will be made without undue delay and dependent on the circumstances, be made before the supervisory authority is notified.
The following information will be provided when a breach is notified to the affected individuals:

- A description of the nature of the breach
- The name and contact details of the Data Protection Officer, where more information can be obtained
- A description of the likely consequences of the personal data breach and
  a description of the measures taken, or proposed to be taken, to deal with the personal data breach, including, where appropriate, the measures taken to mitigate any possible adverse effects

*Record of breaches*

The Company records all personal data breaches regardless of whether they are notifiable or not as part of its general accountability requirement under GDPR. It records the facts relating to the breach, its effects and the remedial action taken. As stated earlier in the guidance, all breaches are recorded in the Data Breach Log.

## 11. Complaints

If you believe that your data protection rights may have been breached, and we have been unable to resolve your concern, you may lodge a complaint to the applicable supervisory authority or to seek a remedy through the courts. Please visit https://ico.org.uk/concerns/ for more information on how to report a concern to the UK Information Commissioner's Office.

## 12. External Support from ICO

You can contact ICO for further information, advice and guidance.

https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/