

## **DATA PROTECTION POLICY**

### **1. Policy Statement**

cHRysos HR Solutions Ltd. needs to keep certain information about its employees, learners, apprentices, and other persons to allow it to monitor progress, achievements, equality and health and safety. To comply with the law, information must be collected and used fairly, stored safely and not disclosed to any other person unlawfully.

The organisation is committed to being transparent about how it collects and uses the personal data of its workforce, and to meeting its data protection obligations. This policy sets out the organisation's commitment to data protection, and individual rights and obligations in relation to personal data.

The organisation has appointed Sheila Moore, Managing Director as its data protection officer. Their role is to inform and advise the organisation on its data protection obligations. Questions about this policy, or requests for further information, should be directed to the data protection officer.

### **2. General Principles**

The management of information by cHRysos HR must comply with the Data Protection Principles which are set out in the Data Protection Act 1998 (the 1998 Act), General Data Protection Regulations and any subsequent amendments. In summary these state that personal data shall:

- be obtained and processed transparently, fairly, and lawfully and shall not be processed unless certain conditions are met
- be obtained for a specified and lawful purpose and shall not be processed in any manner incompatible with that purpose
- be adequate, relevant, and not excessive for those purposes
- be accurate and kept up to date
- not be kept longer than is necessary for the purpose
- be processed in accordance with the data subject's rights
- be kept safe from unauthorised access, accidental loss, or destruction
- not be transferred to a country outside the European Economic Area unless that country has equivalent levels of protection for personal data.

This policy has been produced to ensure that cHRysos HR follows these principles.

### **3. Scope**

This policy applies to employees, associates, learners, apprentices, and other users of cHRysos HR Solutions Ltd.

### **4. Policy**

#### **4.1. Notification of Data Held and Processed**

All staff, associates, apprentices, learners and other users are entitled to:

- know what information the organisation holds and processes about them and why
- know how to gain access to it
- know how to keep it up to date
- know what the organisation is doing to comply with its obligations under the 1998 Act.

The organisation will therefore notify all staff, learners, apprentices, and other relevant users of the types of data the organisation holds and processes about them, and the reasons for which it is processed. The organisation will endeavour to do this at least once every two years.

#### **4.2. Responsibility of Staff**

All staff are responsible for:

- checking that any information that they provide to the organisation in connection with their employment is accurate and up to date
- informing the organisation of any changes to personal data, which they have provided
- checking the information that the organisation will send out to them from time to time, advising of the data that is kept and processed about them
- informing the organisation of any errors or changes. The organisation cannot be held responsible for any errors unless the staff member has informed the organisation of them.

Appendix 1 sets out guidelines for data protection.

#### **4.3. Information Security Procedure**

All staff are responsible for ensuring that:

- any personal data which they hold is kept securely
- personal information is not disclosed either orally or in writing or accidentally or otherwise to any unauthorised third party.

Personal information should be:

- kept in a locked filing cabinet; or
- in a locked drawer; or
- if it is computerised, be password protected; or
- kept only on a disk or memory stick which is itself kept securely.

Where the organisation engages third parties to process personal data on its behalf, such parties do so on the basis of written instructions, are under a duty of confidentiality and are obliged to implement appropriate technical and organisational measures to ensure the security of data.

#### **4.4. Learner Obligations**

Learners (including apprentices) should ensure that all personal data provided to the organisation is accurate and up to date. They must ensure, for example, that changes of address are notified to the Business Support and Customer Services Assistant.

#### **4.5. Information Rights Procedure**

To make a subject access request, the individual should send the request to [email address] or use the organisation's form for making a subject access request. In some cases, the organisation may need to ask for proof of identification before the request can be processed. The organisation will inform the individual if it needs to verify their identity and the documents it requires.

The organisation will normally respond to a request within a period of one month from the date it is received. In some cases, such as where the request is complex, it may respond within three months of the date the request is received. The organisation will write to the individual within one month of receiving the original request to tell them if this is the case.

If a subject access request is manifestly unfounded or excessive, the organisation is not obliged to comply with it. Alternatively, the organisation can agree to respond but will charge a fee, which will be based on the administrative cost of responding to the request. A subject access request is likely to be manifestly unfounded if it is made with the intention of harassing the organisation or causing disruption, or excessive where it repeats a request to which the organisation has already responded. If an individual submits a request that is unfounded or excessive, the organisation will notify them that this is the case and whether it will respond to it.

#### **4.6. Other rights**

Individuals have a number of other rights in relation to their personal data. They can require the organisation to:

- rectify inaccurate data;
  - stop processing or erase data that is no longer necessary for the purposes of processing;
  - stop processing or erase data if the individual's interests override the organisation's legitimate grounds for processing data (where the organisation relies on its legitimate interests as a reason for processing data);
  - stop processing or erase data if processing is unlawful; and
  - stop processing data for a period if data is inaccurate or if there is a dispute about whether the individual's interests override the organisation's legitimate grounds for processing data.
- To ask the organisation to take any of these steps, the individual should send the request to [email address].

#### **4.7. Sensitive Data and Subject Consent**

In many cases, the organisation may only process personal data with the consent of the individual and in the case of sensitive data, express consent must be obtained.

Where the organisation processes special categories of personal data or criminal records data to perform obligations, to exercise rights in employment law, or for reasons of substantial public interest, this is done in accordance with legislation on processing special categories of data and criminal records data.

Any information about a living individual that includes facts, intentions, or opinions about any of the following matters is sensitive data for the purposes of The Act:

- Race or ethnic origin
- Political beliefs
- Religious or other beliefs
- Whether or not someone is a member of a trade union
- Sexual life
- Physical or mental health condition
- The committing or alleged committing by a person of an offence
- Any proceedings for an offence committed

Learners will be asked to sign their consent to process particular types of information when enrolling on a course.

The organisation may also ask for information about particular health needs, such as allergies to particular forms of medication, or conditions such as asthma or diabetes. The organisation will only use this information in the protection of the health and safety of the individual but will need consent to process in the event of a medical emergency.

#### **4.8. Retention of Data**

The organisation will keep some forms of information for longer than others. Information about learners and apprentices will not be kept indefinitely unless there are specific requests to do so. In general, information about learners and apprentices will be kept for a maximum of 3 years after they have completed a course. This will include:

- name and address
- achievements, including assessment decisions
- copies of any references written
- enrolment on course information

The addendum at Appendix 2 provides specific information about the management of data in relation to work-based learners, their portfolios and candidate records.

The organisation will need to keep information about staff for longer periods of time. In general, all information will be kept for 7 years after a member of staff leaves the organisation. Some information will need to be kept for much longer. This will include information necessary in respect of taxation, potential or current

disputes or litigation regarding the employment and information required for job references.

#### **4.9. Data Breach Reporting Procedure**

Although cHRySOS HR takes measures against unauthorised or unlawful processing and against accidental loss, destruction or damage to personal data as set out in this policy, a data security breach could still happen.

Examples of data breaches include:

- Loss or theft of data or equipment on which data is stored (e.g., losing an unencrypted USB stick, losing an unencrypted mobile phone)
- Inappropriate access controls allowing unauthorised use
- Equipment failure
- Human error (e.g., sending an email to the wrong recipient)
- Information posted to the wrong address, dropping/leaving documents containing personal data in a public space)
- Unforeseen circumstances such as fire or flood
- Hacking attack
- 'Blagging' offences where information is obtained by deceiving the organisation

Where a breach has occurred, the following steps should be taken immediately:

- The individual who has identified the breach has occurred must notify the Data Protection Officer and complete the Data Breach Notification Form (Appendix 3 – Part A).
- The Data Protection Officer will identify any steps that can be taken to contain the data breach, e.g., Changing passwords and will liaise with team members to action this.
- They will establish whether any steps can be taken to recover any losses and limit the damage the breach could cause (e.g., physical recovery of equipment, back up to restore lost or damaged data)
- Before deciding on the next course of action, the DDC will assess the risks associated with the data breach considering the following and complete Data Breach Notification Form (Appendix 3 – Part C):
  - What type of data is involved?
  - How sensitive is it?
  - If data has been lost/stolen, are there any protections in place such as encryption?
  - What has happened to the data?
  - What could the data tell a third party about the individual?
  - How many individuals' data have been affected by the breach?
  - Whose data has been breached?
  - What harm can come to those individuals?

- Are there wider consequences to consider such as reputational loss?
- Following the risk assessment in step 4, the Data Protection Officer should notify the ICO within 72 hours of the identification of a data breach if it is deemed that the breach is likely to have a significant detrimental effect on individuals. This might include if the breach could result in discrimination, damage to reputation, financial loss, loss of confidentiality or any significant economic or social disadvantage.
- The Data Protection Officer should contact ICO and record the details of this contact.
- They must assess whether it is appropriate to notify the individual(s) whose data has been breached. If it is determined that the breach is likely to result in a high risk to the rights and freedoms of the individual(s) then they must be clearly expressed.
- The Data Protection Officer will assess whether any changes need to be made to cHRysos HR processes and procedures to ensure that a similar breach does not occur and complete Part D of the Data Breach Notification Form (Appendix 3 – Part D).

**4.10. Monitoring and Review**

The Data Protection Policy will be reviewed biennially or when QCA or legislative changes occur.


**4.11. Responsibility**

Compliance with the 1998 Act and GDPR is the responsibility of all members of the organisation.

**4.12. Training**

The organisation will provide training to all individuals about their data protection responsibilities as part of the induction process and at regular intervals thereafter.

Individuals whose roles require regular access to personal data, or who are responsible for implementing this policy or responding to subject access requests under this policy, will receive additional training to help them understand their duties and how to comply with them.

Author	Sheila Moore
Position	Manging Director
Last reviewed	April 2024
Date for next review	April 2026
Signature	

**Appendix 1**

**STAFF GUIDELINES FOR DATA PROTECTION**

- 1 Staff process data about learners/apprentices on a regular basis when enrolling, writing assessment reports etc. The organisation will ensure through enrolment procedures that all learners/apprentices give their consent to this processing and are notified of the categories of processing as required by the 1998 Act and GDPR. The information that staff deal with on a day-to-day basis will be “standard” and will cover categories such as:
  - general personal details such as name and address
  - details about assessment decisions and associated comments
  - notes of personal tutorials
  
- 2 Information about a learner’s physical or mental health; sexual life; political or religious views; trade union membership, ethnicity or race is sensitive and can only be collected and processed with the individual’s consent. For example, recording information about dietary needs, for religious or health reasons; recording information that a learner is pregnant to ensure appropriate pastoral care or health and safety.
  
- 3 All staff have a duty to ensure that records are:
  - accurate
  - up to date
  - fair
  - kept and disposed of safely, and in accordance with the organisation’s policy
  
- 4 As the Designated Data Controller, the Managing Director is the only member of staff authorised to hold or process data that is:
  - not standard data; or
  - sensitive data

The only exception to this will be if a non-authorised member of staff is satisfied that the processing of the data is necessary:

- in the best interests of the learner, apprentice, or staff member, or a third person, or the organisation; AND
- he or she has either informed the Managing Director or has been unable to do so and processing is urgent and necessary in the circumstances.

This should only happen in very limited circumstances. For example, a learner is injured and unconscious but in need of medical attention and a staff member tells

the hospital that the learner/apprentice is pregnant or a Jehovah's Witness. Action taken in circumstances of this nature should be reported to the Managing Director.

- 5 All staff will be responsible for ensuring that all data is kept securely.
- 6 Staff shall not disclose personal data to any other staff members except with the authorisation or agreement of the Designated Data Controller, or in line with cHRysos HR policy.
- 7 Before processing any personal data, all staff should consider the following checklist:
  - Do you really need to record the information?
  - Is the information "standard" or sensitive?
  - If it is sensitive, do you have the data subject's express consent?
  - Has the individual been told that this type of data will be processed?
  - Are you authorised to collect/store/process the data?
  - If yes, have you checked with the data subject that the data is accurate?
  - Are you sure that the data is secure?
  - If you do not have the data subject's consent to process, are you satisfied that it is in the best interests of the learner or staff member to collect and retain the data?
  - Have you reported the fact of data collection to the authorised person?



**ADDENDUM TO DATA PROTECTION POLICY**

**MANAGEMENT OF INFORMATION**

**Recording and Retention of Data**

All assessment activity and decisions relating to learners undertaking a work-based learning or apprenticeship programme must be recorded using the standard documentation.

A copy of the completed assessment documentation must be kept in the learner's electronic file.

Assessment documentation will be kept on file, stored securely, for 3 years after certification, in line with the requirements of our awarding bodies.

**Access to Information**

Assessment documentation must be made available to the Centre Development Executive/CIPD Moderation Team/OFSTED when requested but must not be disclosed to any individual without a right to access it.

Learners/apprentices have a right to access all documentation relating to their assessment.

Learners/apprentices are entitled to and will be given confidentiality in respect of their evidence and assessment outcomes. Portfolios will not be shared with other learners without prior permission.

Data Breach Incident Form

Part A: Breach Information

When did the breach occur (or become known)?	
Which staff member was involved in the breach?	
Who was the breach reported to?	
Date of Report:	
Time of Report:	
Description of Breach:	
Initial Containment Action taken:	

Part B: Breach Risk Assessment

What type of data is involved?	Hard Copy: Yes/No Electronic Data: Yes/No
Is the data categorised as 'sensitive' within one of the following categories?	Racial or ethnic origin: Yes/No Political opinions: Yes/No Religious or philosophical beliefs: Yes/No Trade union membership: Yes/No Data concerning health or sex life and sexual orientation: Yes/No Genetic data: Yes/No Biometric data: Yes/No
Were any protective measures in place to secure the data (e.g., encryption)?	Yes/No If yes, please outline:
What has happened to the data?	
What could the data tell a third party about the individual?	

<b>Number of individuals affected by the breach:</b>	
<b>Whose data has been breached?</b>	
<b>What harm can come to those individuals?</b>	
<b>Are there wider consequences to consider e.g., reputational loss?</b>	

<b>Is the breach likely to result in a risk to people's rights and freedoms?</b>	Yes/No If yes, then the ICO should be notified within 72 hours.
<b>Date ICO notified:</b>	
<b>Time ICO notified:</b>	
<b>Reported by:</b>	
<b>Method used to notify ICO:</b>	
<b>Notes:</b>	
<b>Is the breach likely to result in a <u>high</u> risk to people's rights and freedoms?</b>	Yes/No If yes, then the individual should be notified
<b>Date individual notified:</b>	
<b>Notified by:</b>	
<b>Notes:</b>	

**Part D: Breach Action Plan**

<b>Action to be taken to recover the data:</b>	
<b>Notification to any other relevant external agencies:</b>	External agencies:
	Date Notified:
<b>Internal procedures (e.g., disciplinary investigation) to be completed:</b>	
<b>Steps needed to prevent reoccurrence of breach:</b>	