

## **DATA PROTECTION POLICY**

### **Policy Statement**

cHRySOS HR Solutions Ltd. needs to keep certain information about its employees, learners 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.

### **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.

### **Scope**

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

### **Policy**

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

All staff, 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 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.

### **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.

### **Data Security**

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.

### **Learner Obligations**

Learners 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 Student Services Officer.

### **Rights to Access Information**

Staff, learners and other users of the organisation have the right to access any personal data that is being kept about them either on computer or on file. Any person who wishes to exercise this right should notify the Managing Director in writing. The data will be made available within 21 days, unless there is good reason for delay in which case, the person making the request will be notified of the reason for the delay.

### **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.

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.

### **The Data Controller and the Designated Data Controller**

chRysos HR Solutions Ltd. is the data controller under the Data Protection regulations. On a day to day basis, the Designated Data Controller is the Director, Service Delivery.

### **Retention of Data**

The organisation will keep some forms of information for longer than others. Information about learners will not be kept indefinitely, unless there are specific

requests to do so. In general, information about learners 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.

### **Monitoring and Review**

The Data Protection Policy will be reviewed on an annual basis or when QCA or legislative changes occur.

### **Responsibility**

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

## **STAFF GUIDELINES FOR DATA PROTECTION**

- 1 Staff process data about learners on a regular basis when enrolling, writing assessment reports etc. The organisation will ensure through enrolment procedures that all learners 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 Director, Service Delivery 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 or staff member, or a third person, or the organisation; AND
- he or she has either informed the Director, Service Delivery 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 is pregnant or a Jehovah's Witness. Action taken in circumstances of this nature should be reported to the Director, Service Delivery or 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  
RELEVANT TO WORK-BASED LEARNERS**

**Recording and Retention of Data**

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

A copy of the completed assessment documentation must be kept in the learner's personal file. The learner will be asked to retain a copy of the assessment report in the front of their portfolio.

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 EQA/OFSTED when requested but must not be disclosed to any individual without a right to access it.

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

Learners 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.