DATA PROTECTION POLICY

Policy adopted by RISE Learning Zone: 01.09.2015

Last reviewed: September 2018

Next review: September 2020

Policy Document OP-06

RISE LEARNING ZONE

DATA PROTECTION POLICY

INTRODUCTION

RISE has a responsibility to ensure that personal information about employees is kept confidential.

In the course of your work you may come into contact with or use confidential information about employees, clients and customers (for example their names and home addresses, medical conditions, payment methods, etc.,).

The **Data Protection Act 1998** (hereafter called the DPA in this document) contains principles affecting all personal data. Information protected by the Act includes not only personal data held on computer but also manual records containing personal data, for example employee personnel files or residents records that form part of a structured filing system.

Also, images of people are covered by the DPA and so is information about people which is derived from images – for example, vehicle registration numbers.

Uses of CCTV by most organisations or businesses will be covered by the Act, regardless of the number of cameras or how sophisticated the equipment is.

The following is explained in more detail below but even at this stage, it is worth noting that it is the responsibility of the EMPLOYER to produce policies, training and advice regarding Data Protection as well as the tools necessary to maintain compliance with the Act (lockable filing cabinets, I.T. Infrastructure, shredders, etc.).

It is the responsibility of the EMPLOYEE to undertake working methods that comply with the Act, otherwise it will be the EMPLOYEE whom will be criminally liable following the breach of the Act.

A breach of data protection is also a disciplinary offence and will be dealt with under the Organisation's disciplinary procedures.

If you access another employee's personnel records without authority, this constitutes a gross misconduct offence and could lead to your summary dismissal.

The RISE Code of Conduct states "information about specific service users, applicants, colleagues, other individuals and commercially or legally sensitive information must never be shared with a third party unless the employee has express permission as part of their role."

Furthermore, there are matters relating to the business and functioning of RISE (e.g. the investigation of complaints or internal consultation about future plans for the organisation) which must also be kept confidential.
If you are in any doubt about what you can or cannot disclose and to whom, do not disclose the information until you have sought further advice from your line manager, or preferably, the Organisation's Data Protection Officer.
In such cases, you are advised that you obtain a contact name and number from anyone seeking information and then check with the Data Protection Officer as to whether you may proceed with the disclosure.

STORAGE AND MOVEMENT OF INFORMATION

STORAGE

Documents containing personal or private information must be securely locked away (not left on desks or in unattended offices) and access to documentation restricted to only those who need to have access. This includes residents, gym members, Children's Services users and discs containing CCTV footage.
Personal and private information should only be divulged on a need to know basis, whether this is internally between staff, session workers and volunteers or to external agencies.
Where statistics are maintained for monitoring and/or marketing, e.g. funding monitoring, etc., this must be done in such a way as to maintain the confidentiality of the individual(s) wherever possible.
Whilst RISE will do all it can to ensure confidentiality is not breached, it is limited in the action it can take in response to breaches of confidentiality away from Organisation premises and/or by people no longer having contact with the organisation.
Data stored on servers is encrypted and secure.
Data stored on 'external storage devices' (hard drives, flash sticks, pen drives, etc.) must also be encrypted. Flash sticks must be YMCA obtained devices, as the protection of the data has been researched with these devices.
RISE has appropriate storage devices and will issue them on a temporary or permanent basis where appropriate.
Consideration is currently being given to a data movement log, where completion of a record will be necessary prior to undertaking any movement of RISE data. Should this be implemented, this policy will be updated to reflect this and managers will be

issued with the new policy.

MOVEMENT (COPY AND/OR TRANSFER)

Prior to moving any data from location to location via any method (physically or via electronic transfer), ensure that it is:

absolutely necessary
only the information that is needed - do not move data that does not need to be moved
safe to do so
done so using lockable storage units whenever possible
done so using RISE issued and configured encrypted storage devices
done so using routers with appropriate security methods (firewalls, encryption, etc).
Data transfers that take place from RISE sites using our routers already have firewalls and all links send and receive data using appropriate levels and types of encryption methods.

Having data intercepted or lost is a matter of great concern for RISE and it should be noted that it is treated very seriously.
Disciplinary action may result from non-compliance with regulations relating to this.

THE DATA PROTECTION PRINCIPLES

There are eight data protection principles that form the main structure of the Act. The Organisation and all its employees must comply with these principles at all times in its information-handling practices.
In brief, the principles say that personal data must be:
1. *Processed fairly and lawfully* and must not be processed unless certain conditions are met in relation to personal data and additional conditions are met in relation to sensitive personal data.
The conditions are either that the person in question has given consent to the processing, or the processing is necessary for the various purposes set out in the Act. Sensitive personal data may only be processed with the explicit consent of the person in question and consists of information relating to:

- race or ethnic origin
- political opinions and trade union membership

- religious or other beliefs
- physical or mental health or condition
- sexual life
- criminal offences both committed and alleged.

2. *Obtained only for one or more specified and lawful purposes* and not processed in a manner incompatible with those purposes. This means that at least one specified reason for processing must be justified. There may be many reasons but there must be at least one.
3. *Adequate, relevant and not excessive*. The Organisation will review personnel files on an annual basis to ensure they do not contain a backlog of out-of-date information and to check there is sound business reason requiring information to continue to be held.
4. *Accurate and where necessary, kept up-to-date*.
If your personal information changes, for example you change address, you must inform your line manager as soon as practicable so that the Organisation's records can be updated. The Organisation cannot be held responsible for any errors unless you have notified the Organisation of the relevant change. In the same way, if data is processed, the updating of the details should take place where appropriate.
5. *Not kept for longer than is necessary.* The Organisation will keep personnel files for no longer than six years after termination of employment. Different categories of data will be retained for different time periods, depending on legal, operational and financial requirements. Any data which the Organisation decides it does not need to hold for a period of time will be destroyed after six months. Data relating to unsuccessful job applicants will only be retained for a period of six months unless permission has been obtained to retain information.
6. *Processed appropriately* in accordance with the rights of employees under the Act. Processing means any use of the data including (but not limited to) storage, viewing (use) and disposal.
7. *Handled with appropriate technical and organisational measures in place*.
Secure, technical and organisational measures will be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, data.
Data stored on removable media will be kept in locked filing cabinets.
Data held on computer will be stored confidentially by means of password

protection, encryption or coding and again only authorised employees shall have access to that data. The Organisation has network backup procedures to ensure that data on computer cannot be accidentally (or intentionally) lost or destroyed. Paper-based Personnel files are confidential and are stored in locked filing cabinets. Only authorised staff have access to these files.
Files will not be removed from their normal place of storage without good reason.

8. *Not transferred to a country or territory outside the European Economic Area unless* that country ensures an adequate level of protection for the processing of personal data.
This means not sharing (or even taking to or storing) data (including anonymous statistical data) with any other country or territory outside the European Economic Area unless that country or territory ensures an adequate level of protection for the processing of personal data.

YOUR CONSENT TO PERSONAL INFORMATION BEING HELD
The Organisation holds personal data about you and by signing your contract of employment, starter form, return to work form, etc., you have consented to that data being processed by the Organisation.
Obviously, it is vital that we store information about you (Bank details for payroll, etc.,) and therefore, agreement to the Organisation processing your personal data is a condition of your employment.
The Organisation also holds limited sensitive personal data about its employees and by signing your contract of employment, you give your explicit consent to the Organisation's holding and processing of that data, for example sickness absence records, health needs and equal opportunities monitoring data.

YOUR RIGHT TO ACCESS PERSONAL INFORMATION
You have the right, on request, to receive a copy of the personal information that the Organisation holds about you, including your personnel file and to demand that any inaccurate data be corrected or removed.
This pertains to any organisation that stores information about you.

You have the right on request:

to be told by the Organisation for what purpose(s) personal data about you is being processed
to be given a description of the data held about you and the recipients to whom it may be disclosed
to have communicated to you the personal data concerned and any information available as to the source of the data
to be informed of the logic involved in the decision-making concerning computerised processing.

Upon request, with notice, the Organisation will allow you access to your personnel file. If you wish to make a copy of any personal data held about you, you should make a written request for this and the Organisation reserves the right to charge an administration fee of up to £15.
If you wish to make a complaint that these rules are not being followed in respect of personal data the Organisation holds about you, you should raise the matter with the Data Protection Officer.
If the matter pertains to the Data Protection Officer or is not resolved to your satisfaction, it should be raised as a formal grievance under the Organisation's grievance procedure.

YOUR OBLIGATIONS IN RELATION TO PERSONAL INFORMATION

You should ensure you comply with the following guidelines at all times: You MUST

- · not give out confidential personal information except to the data subject. In particular, it should not be given to someone from the same family or to any other unauthorised third party unless the data subject has given their explicit consent to this
- · be aware that those seeking information sometimes use deception in order to gain access to it - always verify the identity of the data subject and the legitimacy of the request, particularly before releasing personal information by telephone
- · forward any requests for personal information about another employee to the HR team who will be responsible for dealing with such requests
- · always log off (or 'lock') your computer when you are temporarily leaving your work station and never give out your password (an exception to this is when the I.T. Support company are attempting to rectify an issue). Once the

problem has been rectified, it is recommended that you subsequently change your password

- · always keep office doors locked if the office is to be unoccupied
- · not present/display confidential information in areas where other employees/service

users/contractors/other agencies have access (e.g. contact details for staff, etc.)

- · understand that compliance with the Act is YOUR responsibility. If you have any questions or concerns about the interpretation of these rules, take this up with the

Data Protection Officer.

- · Book meeting rooms to conduct business so that others may operate in their normal

working environments without compromising personal data.

STEPS RISE HAVE TAKEN

RISE regularly review the guidance offered by the Information Commissioner's Office (ICO (who are responsible for the concept, review and implementation of the Data Protection Act)) to help ensure that we consider the latest legislation and recommendations.

With regard to Data and Computer Security, we have already put in place all of the recommendations that the ICO have issued, including encryption and the backing up of data. We do not seek to keep CCTV footage for longer than one calendar month, unless evidence of an activity is required by us or the Police with regard to an on-going investigation.

Our policies are written and reviewed with the DPA in mind to help maintain compliance with the Act.

FREEDOM OF INFORMATION ACT

You may have heard of this Act as it is mentioned in the media on a regular basis. Although only Local Authorities and some statutory bodies (NHS Trust, Police, etc.,) are bound to this Act, we currently have contracts with some of these bodies that are bound to the Act.

Therefore, if you are asked for any information regarding the Freedom Of Information (or FOI) Act, you must contact the Data Protection Officer immediately.

Should the Data Protection Officer be absent, contact a member of the Executive Management Team (Heads of H.R. and Finance, or the Programmes Director or the Chief Executive) immediately.

TRAINING & ADVICE

Data Protection training is compulsory for ALL employees and as such, if you have not undertaken this training, you should inform HR immediately.

If you have any other queries or comments regarding this policy, please contact the Chair of Directors: Martin Sumner