Park College

Data Protection Policy

Author & Owner: The Park Community Centre Ltd and Park Education Ltd

Contact: HR department. Tel: 0117 9039770

Date Adopted 26/07/2016

Date Reviewed: 11/12/2018

Reviewed: 17/01/2021

Date reviewed 15/03/2023

Date reviewed 2/04/2025

Date to be reviewed 2/4/2027

The audience of this document is made aware that a physical copy may not be the latest available version, which supersedes all previous versions. This is available from the HR department at the Park Community Centre Ltd.

Those to whom this policy applies are responsible for familiarising themselves periodically with the latest version and for complying with policy requirements at all times.

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. The **Data Protection Act 1998** contains principles affecting employees' and other personal records. Information protected by the Act includes not only personal data held on computer but also certain manual records containing personal data, for example employee personnel files that form part of a structured filing system. The purpose of these rules is to ensure you do not breach the Act. If you are in any doubt about what you can or cannot disclose and to whom, do not disclose the personal information until you have sought further advice from Emma Hinton, The Company's Data Protection Officer. You should be aware that you can be criminally liable if you knowingly or recklessly disclose personal data in breach of the Act. A serious breach of data protection is also a disciplinary offence and will be dealt with under our 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.

Park College

The data protection principles

There are eight data protection principles that are central to the Act. All of our 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 employee 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 employee 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.

3. Adequate, relevant and not excessive. We 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 a sound business reason requiring information to continue to be held.

4. Accurate and 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 our records can be updated. We cannot be held responsible for any errors unless you have notified us of the relevant change.

5. Not kept for longer than is necessary. We 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 we decide does not need to held for a period of time will be destroyed after one year. Data relating to unsuccessful job applicants will only be retained for a period of one year.

6. Processed in accordance with the rights of employees under the Act.

7. Appropriate 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, personal data. Personnel files are confidential and are stored in locked filing cabinets. Only authorised employees have access to these files. Files will not be removed from their normal place of storage without good reason. Personal data stored on discs, memory sticks, portable hard drives or other

removable storage media will be kept in locked filing cabinets or locked drawers when not in use by authorised employees. Data held on computers will be stored confidentially by means of password protection, encryption or coding, and again only authorised employees have access to that data. We have network backup procedures to ensure that data on computers cannot be accidentally lost or destroyed.

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.

Security of data being held

Personal data held by us will always be held in a secure way/environment, protected by password and accessible by authorised personnel. You must not move such data out of a secure environment or store it, or any personal data you may have accessed, gathered or downloaded in such a way as might make it accessible to unauthorised persons. All personal data must be protected by password and that password must be changed on a regular basis.

Your consent to personal information being held

We hold personal data about you and, by signing your contract of employment, you have consented to that data being processed by ourselves. Agreement to our processing your personal data is a condition of your employment. We also hold limited sensitive personal data about our employees and, by signing your contract of employment, you give your explicit consent to the 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 we hold about you, including your personnel file, and to demand that any inaccurate data be corrected or removed. You have the right on request:

- to be told by ourselves whether and for what purpose personal data about you is being processed
- to be given a description of the data and the recipients to whom it may be disclosed
- to have communicated in an intelligible form the personal data concerned, and any information available as to the source of the data
- to be informed of the logic involved in computerised decision-making.

Upon request, we will provide you with a statement regarding the personal data held about you. This will state all the types of personal data we hold and processes about you and the reasons for which they are processed. If you wish to access a copy of any personal data being held about you, you must

make a written request for this and we reserve the right to charge you a fee of up to £10. To make a request, please complete a Personal Data Subject Access Request Form, which can be obtained from the Data Protection Officer.

If you wish to make a complaint that these rules are not being followed in respect of personal data we hold about you, you should raise the matter with the Data Protection Officer. If the matter is not resolved to your satisfaction, it should be raised as a formal grievance under our grievance procedure.

Your obligations in relation to personal information

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

- do 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
- only transmit personal information between locations by fax or e-mail if a secure network is in place, for example, a confidential fax machine or encryption is used for e-mail
- if you receive a request for personal information about another employee, you should forward this to The Data Protection Officer who will be responsible for dealing with such requests, this includes references for employees/ ex-employees; you may never provide a company based reference and all requests for references should be forward to The Data Protection Officer
- ensure any personal data you hold is kept securely, either in a locked filing cabinet or, if computerised, it is password protected
- 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.

Security

As many computer files contain some form of confidential or otherwise sensitive business information, we take the security of these files very seriously. With this in mind, we have introduced some basic security precautions that all employees must abide by.

These are as follows:

- if you need to leave your computer for more than a couple of minutes, lock the computer screen
- if you need to leave your computer for a long period of time, log off - never leave an unattended computer logged on

- computer passwords are considered our confidential information even if you are using your personal password for social networking to login to our work systems. When creating a computer password, do not use one that is obvious, such as your date of birth or the name of a close family member - passwords should preferably be a mix of letters and numbers and should not be the same as any other personal passwords you may have (such as Internet banking passwords)
- always keep your password private, do not write it down and do not divulge it to anyone else (including other members of staff), except for …… *(insert details)*
- if you suspect that someone knows your password, change it in the normal way
- change your password at regular intervals in any event
- always shut down your computer when you go home at the end of the day
- if you notice any suspicious activity, for example an employee trying to gain unauthorised access to another member of staff's computer, notify your manager immediately
- If you become aware that someone, internally or externally has tried to access your drive(s) or computer you must make NAME/DEPT. aware immediately
- if you are provided with a company computer for use in your home, family members [are/are not] (amend as necessary) allowed to use it
- (insert any other measures)

This Policy is alongside the policies and principles for GDPR.