DATA PROTECTION POLICY

The ELKOLET Centre, Mill Lane, Alton, GU34 1BD

T: 01420 86980 **W:** www.elkolet.com

Reviewer	Paula Knowles
Review Date	September 2024
Next Review Date	September 2025

Contents

INTRODUCTION

We may have to collect and use information about people with whom we work or with students who attend our Alternative Education Provision, The King's Way. This personal information must be handled and dealt with properly, however it is collected, recorded and used, and whether it be on paper, in computer records or recorded by any other means.

We regard the lawful and correct treatment of personal information as very important to our successful operation and to maintaining confidence between us and those with whom we carry out business. We will ensure that we treat personal information lawfully and correctly.

To this end we fully endorse and adhere to the principles of the General Data Protection Regulation (GDPR).

This policy applies to the processing of personal data in manual and electronic records kept by us in connection with our human resources function as described below. It also covers our response to any data breach and other rights under the GDPR.

This policy applies to the personal data of the following:

- job applicants
- existing and former employees
- apprentices
- volunteers
- placement students
- workers
- self-employed contractors
- existing and former students
- prospective students
- parents/guardians of students

These are referred to in this policy as relevant individuals.

DEFINITIONS

"Personal data" is information that relates to an identifiable person who can be directly or indirectly identified from that information, for example, a person's name, identification number, location, online identifier. It can also include pseudonymised data.

"Special categories of personal data" is data which relates to an individual's health, sex life, sexual orientation, race, ethnic origin, political opinion, religion, and trade union membership. It also includes genetic and biometric data (where used for ID purposes).

"Criminal offence data" is data which relates to an individual's criminal convictions and offences.

"Data processing" is any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

DATA PROTECTION PRINCIPLES

Under GDPR, all personal data obtained and held by us must be processed according to a set of core principles. In accordance with these principles, we will ensure that:

a) processing will be fair, lawful and transparent
b) data be collected for specific, explicit, and legitimate purposes
c) data collected will be adequate, relevant and limited to what is necessary for the purposes of processing
d) data will be kept accurate and up to date. Data which is found to be inaccurate will be rectified or erased without delay
e) data is not kept for longer than is necessary for its given purpose
f) data will be processed in a manner that ensures appropriate security of personal data including protection against unauthorised or unlawful processing, accidental loss, destruction or damage by using appropriate technical or organisation measures
g) we will comply with the relevant GDPR procedures for international transferring of personal data

TYPES OF DATA HELD

We keep several categories of personal data on relevant individuals in order to carry out effective and efficient processes. We keep this data in a personnel file relating to each employee and we also hold the data within our computer systems, for example, our holiday booking system.

We hold the following types of data on workers:

a) personal details such as name, address, phone numbers
b) information gathered via the recruitment process such as that entered into a CV or included in a CV cover letter, references from former employers, details on your education and employment history etc
c) details relating to pay administration such as National Insurance numbers, bank account details and tax codes
d) medical or health information
e) information relating to your employment with us, including:
    i) job title and job descriptions
    ii) your salary
    iii) your wider terms and conditions of employment
    iv) details of formal and informal proceedings involving you such as letters of concern, disciplinary and grievance proceedings, your annual leave records, appraisal and performance information
    v) internal and external training modules undertaken

We hold the following types of data on students:

a) sensitive demographic information
    i) race, religious beliefs etc
b) personal information
    i) address, SEND assessments etc
c) academic performance
    i) includes test scores and grades
d) behavioural records

i) attendance
ii) discipline incidents

e) engagement indicators
i) participation in activities

All of the above information is required for our processing activities. More information on those processing activities are included in our privacy notice for employees, which is available from your manager.

RIGHTS OF THE INDIVIDUAL

You have the following rights in relation to the personal data we hold on you:

a) **the right to be informed** about the data we hold on you and what we do with it
   i) privacy notice for workers and students can be found at www.elkolet.com/policy-center ;
b) **the right of access** to the data we hold on you.
   i) More information on this can be found in the section headed "Access to Data";
c) **the right to rectification** for any inaccuracies in the data we hold on you, however they come to light, to be corrected;
d) **the right to erasure** where you may request all Personal Information we have be deleted
   i) we are required to comply with a request for erasure unless we have reasonable ground to refuse
e) **the right to restrict the processing of the data**;
f) **the right to portability**
   i) you have the right to transfer the data we hold on you to yourself or,
   i) another party
g) **the right to object** to the inclusion of any information;
h) **the right to regulate any automated decision-making and profiling of personal data**.

RESPONSIBILITIES

In order to protect the personal data of relevant individuals, those within our business who must process data as part of their role have been made aware of our policies on data protection.

We have also appointed a Data Protection Officer (DPO) with responsibility for reviewing and auditing our data protection systems.

LAWFUL BASES OF PROCESSING

We acknowledge that processing may be only be carried out where a lawful basis for that processing exists and we have assigned a lawful basis against each processing activity.

ELKOLET will, before any processing of Personal Information starts for the first time,
and then regularly while it continues:

a) Process the Personal Information on at least one of the following bases:

i) Consent:

- the individual has given their express agreement to the processing of their Personal Information for one or more specific purposes

- parental consent will be obtained for any child aged under 13 years old or for children aged over 13 who are not considered capable of giving consent themselves;

ii) Contractual:

- the processing is necessary for the performance of a contract to which the individual is party or in order to take steps at the request of the individual prior to entering into a contract;

iii) Legal Obligation:

- the processing is necessary for compliance with a legal obligation to which ELKOLET is subject;

iv) Vital Interests:

- the processing is necessary for the protection of the vital interests of the individual or another natural person; or

v) Public Interest:

- the processing is necessary for the performance of a task carried out in the public interest or exercise of official authority; or

vi) Legitimate Interests:

- the processing is necessary for the purposes of legitimate interests of ELKOLET or a third party, except where those interests are overridden by the interests of fundamental rights and freedoms of the individual, in particular where the individual is a child.

b) except where the processing is based on consent, satisfy ourselves that the processing is necessary for the purpose of the relevant lawful basis (i.e. that there is no other reasonable way to achieve that purpose);

c) document our decision as to which lawful basis applies to help demonstrate our compliance with the data protection principles;

d) include information about both the purposes of the processing and the lawful basis for it in our relevant privacy notices located at www.elkolet.com/policy-center;

b) where Special Category Data is processed, identify a lawful special condition for processing that information and document it; and

c) where criminal offence information is processed, identify a lawful condition for processing that information and document it.

ACCESS TO DATA

As stated above, relevant individuals have the right to access personal data that we hold on them. To exercise this right, employees parents/guardians students etc, should make a Subject Access Request. We will comply with the request without delay, and within one month unless, in accordance with legislation, we decide that an extension is required. Those who make a request will be kept fully informed of any decision to extend the time limit.

No charge will be made for complying with a request unless the request is manifestly unfounded, excessive or repetitive, or unless a request is made for duplicate copies to be provided to parties other than the employee making the request. In these circumstances, a reasonable charge will be applied.

Further information on making a subject access request is contained in our Subject Access Request policy.

DATA DISCLOSURES

The Company may be required to disclose certain data/information to any person. The circumstances leading to such disclosures include:

a) any employee benefits operated by third parties;
b) disabled individuals - whether any reasonable adjustments are required to assist them at work;
c) individuals' health data - to comply with health and safety or occupational health obligations towards the employee;
d) for Statutory Sick Pay purposes;
e) HR management and administration - to consider how an individual's health affects his or her ability to do their job;
f) the smooth operation of any employee insurance policies or pension plans;
g) to assist law enforcement or a relevant authority to prevent or detect crime or prosecute offenders or to assess or collect any tax or duty.
h) referral to relevant support services e.g. social services, CAMHS

These kinds of disclosures will only be made when strictly necessary for the purpose.

DATA SECURITY

All our employees are aware that hard copy personal information should be kept in a locked filing cabinet, drawer, or safe.

Employees are aware of their roles and responsibilities when their role involves the processing of data. All employees are instructed to store files or written information of a confidential nature in a secure manner so that are only accessed by people who have a need and a right to access them and to ensure that screen locks are implemented on all PCs, laptops etc when unattended. No files or written information of a confidential nature are to be left where they can be read by unauthorised people.

Where data is computerised, it should be coded, encrypted or password protected both on a local hard drive and on a network drive that is regularly backed up. If a copy is kept on removable storage media, that media must itself be kept in a locked filing cabinet, drawer, or safe.

Employees must always use the passwords provided to access the computer system and not abuse them by passing them on to people who should not have them.

Personal data relating to relevant individuals should not be kept or transported on laptops, USB sticks, or similar devices, unless prior authorisation has been received. Where personal data is recorded on any such device it should be protected by:

a) ensuring that data is recorded on such devices only where absolutely necessary.
b) using an encrypted system — a folder should be created to store the files that need extra protection and all files created or moved to this folder should be automatically encrypted.
c) ensuring that laptops or USB drives are not left where they can be stolen.

Failure to follow the Company's rules on data security may be dealt with via the Company's disciplinary procedure. Appropriate sanctions include dismissal with or without notice dependent on the severity of the failure.

THIRD PARTY PROCESSING

Where we engage third parties to process data on our behalf, we will ensure, via a data processing agreement with the third party, that the third party takes such measures in order to maintain the Company's commitment to protecting data.

INTERNATIONAL DATA TRANSFERS

The Company does not transfer personal data to any recipients outside of the United Kingdom.

REQUIREMENT TO NOTIFY BREACHES

All data breaches will be recorded on our Data Breach Register. Where legally required, we will report a breach to the Information Commissioner within 72 hours of discovery. In addition, where legally required, we will inform the individual whose data was subject to breach.

More information on breach notification is available in our Breach Management policy.

TRAINING

New employees must read and understand the policies on data protection as part of their induction.

All employees receive training covering basic information about confidentiality, data protection and the actions to take upon identifying a potential data breach.

The nominated data protection officers for the Company are trained appropriately in their roles under the GDPR.

All employees who need to use the computer system are trained to protect relevant individuals' private data, to ensure data security, and to understand the consequences to them as individuals and the Company of any potential lapses and breaches of the Company's policies and procedures.

RECORDS

The Company keeps records of its processing activities including the purpose for the processing and retention periods in its Record of Processing Activities. These records will be kept up to date so that they reflect current processing activities.

DATA PROTECTION COMPLIANCE

Our appointed compliance officer in respect of our data protection activities is:

Angel Knowles