Specialist Education Support Network

Data Protection Policy

Policy issue date: January 2019

Policy review date: January 2020

Data Protection Policy

Introduction

SESN is fully committed to compliance with the requirements of the Data Protection Act 1998 (DPA).

We are required to maintain certain personal data about individuals for the purposes of satisfying our operational and legal obligations. We recognise the importance of correct and lawful treatment of personal data as it helps to maintain confidence in our business and to ensure efficient and successful outcomes when using this data.

The types of personal data that we may process include information about current, past and prospective employees, subcontractors, students, suppliers, partners and other organisations with whom we have dealings.

Personal data may consist of data kept on paper, computer or other electronic media; all of which is protected under the Data Protection Act 1998.

This policy is not contractual but indicates how SESN intends to meet its legal responsibilities for data protection.

Scope of this policy

This policy applies to all employees who handle personal data, whether this relates to their colleagues, students or anyone else. A copy will also be given to any third parties to whom we outsource any data processing.

Aims of this policy

This policy aims to assist employees and management to comply with the requirements of the Data Protection Act 1998 and to minimise any risk to the organisation by setting out clear guidelines relating to the processing, storage and disposal of data.

Definitions

The DPA lays down conditions for the processing of any personal data and makes a distinction between 'personal data' and 'sensitive personal data'.

'Personal data' is defined as data relating to a living individual who can be identified from that data; or from that data and other information which is in the possession of, or is likely to come into the possession of the data controller, and includes an expression of opinion about the individual and any indication of the intentions of the data controller, or any other person, in respect of the individual.

'Sensitive personal data' is defined as personal data consisting of information regarding an individual's racial or ethnic origin; political opinion; religious or other beliefs; trade union membership; physical or mental health or condition; sexual life; or criminal proceedings or convictions.

Principles

We endorse and adhere to the eight principles of the Data Protection Act which are summarised as follows:

Data must:

1. be processed fairly and lawfully and shall not be processed unless certain conditions are met.

2. be obtained for a specified and lawful purpose and shall not be processed in any manner incompatible with that purpose.

3. be adequate, relevant and not excessive for those purposes.

4. be accurate and, where necessary, kept up to date.

5. only be kept for as long as is necessary for the purpose for which it was obtained.

6. be processed in accordance with the data subject's rights.

7. be kept secure from unauthorised or unlawful processing and protected against accidental loss, destruction or damage by using the appropriate technical and organisational measure.

8. not be transferred to a country or territory outside the European Economic Area, unless that country or territory ensures an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data.

These principles apply to obtaining, handling, processing, transportation and storage of personal data. Employees of the organisation who obtain, handle, process, transport and store personal data for us must adhere to these principles at all times.

Handling of personal/sensitive information

SESN will, through appropriate management and the use of strict criteria and controls:

- observe fully the conditions concerning the fair collection and use of personal information
- specify the purpose for which information is used
- collect and process information only to the extent that it is needed to fulfil operational needs or legal requirements
- endeavour always to ensure the quality of information used
- not keep information for longer than required (operationally or legally)
- always endeavour to safeguard personal information by physical and technical means (i.e. keeping paper files and other records or documents containing personal/sensitive data in a secure environment; protecting personal data held on computers and computer systems by the use of secure passwords which, where possible, are changed periodically; and ensuring that individual passwords are not easily compromised)
- ensure that personal information is not transferred abroad without suitable safeguards
- ensure that the lawful rights of people about whom the information is held can be fully exercised.

In addition, SESN will ensure that:

- there is someone with specific responsibility for data protection in the business (the designated Data Controller)

- all those who manage and handle personal information understand that they are responsible for following good data protection practice
- all those who manage and handle personal information are trained to do so and appropriately supervised
- a clear procedure is in place to deal with any data access requests (internal or external) that ensures that such enquiries are dealt with promptly and courteously
- methods of handling personal information are regularly assessed and evaluated
- any data sharing is carried out under a written agreement, setting out the scope and limits of the sharing
- any disclosure of personal data will be in compliance with approved procedures.

SESN also has a legal obligation to provide employee liability information to any organisation that our employees are transferring to, in line with the Transfer of Undertakings (Protection of Employment) Regulations (TUPE).

Access to personal data

All individuals who are the subject of personal data held by us are entitled to:

- ask what information we hold about them and why
- ask how to gain access to it
- be informed of how to keep it up to date
- have inaccurate personal data corrected or removed
- prevent us from processing information or request that it is stopped if the processing of such data is likely to cause substantial, unwarranted damage or distress to the individual or anyone else
- require us to ensure that no decision which significantly affects an individual is solely based on an automated process for the purposes of evaluating matters relating to them, such as conduct or performance
- be informed what we are doing to comply with our obligations under the Data Protection Act. This right is subject to certain exemptions which are set out in the Act.

Any person who wishes to exercise this right should make a request in writing to the Director/Head Teacher. We reserve the right to charge the maximum fee payable for each subject access request. If personal details are inaccurate, they will be amended upon request. If by providing this information we would have to disclose information relating to or identifying a third party, we will only do so provided the third party gives consent, otherwise we may edit the data to remove the identity of the third party.

Unless we are under a legal obligation to release data, or the individual has given us permission, personal information will only be released to the individual to whom it relates.

The disclosure of such information to anyone else without their consent may be a criminal offence. Any employee who is in doubt regarding a subject access request should check with the Director/Head Teacher.

Information must under no circumstances be sent outside of the UK without the prior permission of Management.

SESN aims to comply with requests for access to personal information as quickly as possible, but will ensure that this is provided within 40 days of receipt of a written request unless there is good reason for delay. In such cases, the reason for the delay will be explained in writing to the individual making the request.

Employee responsibilities

All employees must ensure that, in carrying out their duties, SESN is able to comply with its obligations under the DPA/GDPR. In addition, each employee is responsible for:

- checking that any personal data that they provide to us is accurate and up to date
- informing us of any changes to information previously provided, e.g. change of home or email address or phone number, marital status or civil partnership, bank details etc.
- checking any information that we may send out from time to time, giving details of information that is being kept and processed
- ensuring that if, as part of their responsibilities, they collect information about other people or about other employees, they comply with this policy. This includes ensuring that information is processed in accordance with the DPA/GDPR, is only processed for the purposes for which it is held, is kept secure, and is not kept any longer than is necessary.

Employees are reminded that the DPA/GDPR does not just apply to records relating to our employees, but also to the records of any student and their relatives or those who act on their behalf. The information stored should be reviewed regularly to ensure it is accurate and up to date. All documents, whether hand written or saved electronically (for example in emails, current or deleted) are potentially disclosable in the event of a request from an employee or student.

Records

We hold personal information about all employees as part of our general employee records. This includes address and contact details, age, date of birth, marital status or civil partnership, educational background, employment application, employment history with SESN, areas of expertise, details of salary and benefits, bank details, performance appraisals and salary reviews, records relating to holiday, sickness and other leave, working time records and other management records. We may receive and/or retain this information in various forms (whether in writing, electronically, verbally or otherwise).

This information is used for a variety of administration and management purposes, including payroll and benefits administration, facilitating the management of work and employees, performance and salary reviews, complying with record keeping and other legal obligations.

We also process information relating to employees' health, some of which may fall under the definition of 'sensitive personal data'. This typically includes pre-employment health questionnaires; records of sickness absence and medical certificates (including self-certification of absence forms); field work assessments; VDU assessments; noise assessments and any other medical reports.

This information is used to administer contractual and Statutory Sick Pay, monitor and manage sickness absence and comply with our obligations under health and safety legislation and the Working Time Regulations.

From time to time we may ask employees to review and update the personal information we hold about them. We ask that they do not wait until asked to update this information, but inform us immediately of any significant change(s).

Data security

The need to ensure that data is kept securely means that precautions must be taken against physical loss or damage, and that both access and disclosure must be restricted.

All hard copy files are kept in a locked cabinet in the Director's office and are not to be removed. Other information that is stored electronically has appropriate levels of authorisation which prevent unauthorised access.

Data retained on laptops, smartphones and any other electronic equipment that is removed from our offices must be password protected.

All employees are responsible for ensuring that any personal data that they hold is stored securely and that personal information is not disclosed either orally or in writing or otherwise to any unauthorised third party.

References that disclose personal information will not be provided to any third party without the data subject's prior authority (unless this is required or permitted by law such as by the police, HMRC, Contributions Agency or similar body).

Third party processors (such as accountants) will be required to provide sufficient guarantees for their data security measures and compliance with them.

Any employee who discovers personal or sensitive data in an inappropriate place (for example unknowingly sent to the wrong printer) should immediately pass this to their manager/supervisor, ensuring that its contents are not revealed to anyone else.

Publication of information

Information that is already in the public domain is exempt from the Data Protection Act. This would include, for example, information contained within externally circulated publications such as brochures and other sales and marketing literature, or included on our website.

Any individual who has good reason for wishing their details not to be included in such publications should contact their manager/supervisor.

Subject consent

Our contracts of employment agreements require the consent of individuals to the processing of personal data for the purposes of administration, managing and employing them. This includes: payroll, weekly timesheets, benefits, medical records, absence records, sick leave/pay information, performance reviews, disciplinary and grievance matters, pension provision, recruitment, family policies (maternity, paternity, adoption, shared parental leave etc) and equal opportunity monitoring.

Information about an individual will only be kept for the purpose for which it was originally provided. Individuals must not collect data that is simply "nice to have" nor use data for any purpose other than what it was provided for originally.

Retention and disposal of data

Information will be kept in line with our document retention guidelines. All employees are responsible for ensuring that information is not kept for longer than necessary.

Documents containing any personal information will be disposed of securely, and paper copies will be shredded (not disposed of directly into a normal bin or recycling bin).

Information stored on obsolete electronic equipment (desktops, laptops and other devices) will be erased prior to the equipment being sold, disposed of or reallocated to other employees.

Registration

The Data Protection Act 1998/GDPR requires every data controller who is processing personal data, to notify and to renew their notification on an annual basis. Failure to do so is a criminal offence.

SESN is registered in the Information Commissioner's public register of data controllers. Richard Bell is our Data Controller and is responsible for ensuring compliance with the Data Protection Act, for notifying and updating the Information Commissioner of our processing of personal data, and for the monitoring and implementation of this policy on behalf of SESN.

Any changes made to the information stored and processed must be brought to the attention of Richard Bell immediately.

Implementation, monitoring and review of this policy

This policy takes effect immediately. Management has overall responsibility for implementing and monitoring this policy, which will be reviewed on a regular basis and whenever there are relevant changes in legislation or to our working practices.

Any questions or concerns about the interpretation or operation of this policy should be taken up with the Director/Head Teacher. Any breach will be taken seriously and may result in formal disciplinary action. Any employee who considers that the policy has been breached in any way should raise the matter with their manager/supervisor.

Procedures

This procedure may only be amended or withdrawn by the Director of SESN.

Approved by

Signed: ..... Name: ..... Date: .....

Director