Data Protection Policy
Appendix A - GDPR

General Data Protection Regulation

Legal Requirements

Registration

SSC is registered as a Data Controller on the Data Protection Register held by the Information Commissioners Office

Information for Data Subjects (Parents, Employees, clients): PRIVACY NOTICES

In order to comply with the fair processing requirements of the DPA, SSC must inform employees and the parents / carers of all clients of the data they collect, process and hold on the clients, the purposes for which the data is held, the legal basis for holding it and the third parties (e.g. LA, DfE, etc.), and to whom it may be passed. The privacy notice will set out the data subjects' rights under the GDPR.
New privacy notices will be issued to all 'data subjects' even if the data subject has previously received a similar notice.

Introduction

The GDPR defines "personal data" as any information relating to an identified or identifiable natural person (a "data subject"). An identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier, or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural, or social identity of that natural person.

The GDPR also addresses "special category" personal data (also known as "sensitive" personal data). Such data includes, but is not necessarily limited to data concerning the data subject's race, ethnicity, religion, trade union membership, health, sex life, or sexual orientation.

The Homes and the wider Company of SCC collects and uses personal information (referred to in the Data Protection Act 2018 as personal data) about Employees, Young People, parents and other individuals who come into contact with the Young People, the Homes and the Company. This information is gathered in order to enable the provision of care and other associated functions. In addition, the Home and / or Company may be required by law to collect, use and share certain information.
SSC is registered as a Data Controller, with the Information Commissioner's Office (ICO). Details are available on the ICO website.

In accordance with Article 5 of the GDPR, information held will be:

1. Processed lawfully, fairly and in a transparent manner in relation to individuals;
2. Collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall, subject to measures respecting the principle of 'data minimisation', not be considered to be incompatible with the initial purposes;
3. Adequate, relevant and limited to what is necessary in relation to the purpose for which they are processed;
4. Accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay;
5. Kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods

insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes subject to implementation of the appropriate technical and organisational measures required by the GDPR in order to safeguard the rights and freedoms of individuals, and again subject to the 'data minimisation' principle; and

6. Processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisation measures. SSC (the controller) shall be responsible for, and be able to demonstrate, compliance with the principles i.e. its policies and systems comply with requirements of GDPR.

Purpose

This policy sets out how SSC deals with personal information correctly and securely and in accordance with the Data Protection Act 2018 and other related legislation.

This Policy is designed to ensure that our Service sets out the specific purposes for which we hold personal data on Service Users, Employees and Suppliers. The periods for which the data is to be retained, the criteria for establishing and reviewing such periods and when and how it is to be deleted or otherwise disposed of, whilst identifying the practices to be followed in the event of any data breach.
The vast majority of information that SSC will collect and process is required to enable the company to perform tasks carried out in the public interest or in the exercise of official authority vested in the company, as the data controller.

There are other bases that, such as a specific legal obligation applying to the data controller that makes the processing necessary.

Age

Children under the age of 13 are not considered able to give consent to process data or to directly access the rights of a data subject, so parents or guardians do this on their behalf. After the age of 13, this responsibility is transferred to the child and parents will not have responsibility for their child's data.

Consent

If there is a lawful basis for collecting data then consent to collect data is not required. However, a privacy notice which explains to data subjects (or the parents of the data subject if under the age of 10) will be provided. This explains the lawful basis for processing the data, and also explains to the individual their rights.

Parents/Carers of children under the age of 13 will need to give consent when there is not a legal reason for processing, for instance for images used in company publicity or social media feeds. The consent will be transparent, revocable, and will be on a "opt-in" basis.

What is Personal Information/ data?

Personal information or data is information which relates to a living individual who can be identified from that data, or from that data in addition to other information available to them. Personal data includes (but is not limited to) an individual's, name, address, date of birth, photograph, bank details and other information that identifies them.

Rights

The GDPR provides for the following rights:

1. The right to be informed
2. The right of access
3. The right to rectification
4. The right to erasure
5. The right to restrict processing
6. The right to data portability
7. The right to object
8. Rights in relation to automated decision making and profiling

Data Protection Principles

The Data Protection Act 2018 establishes eight principles that must be adhered to at all times:

1. Personal data shall be processed fairly and lawfully;
2. Personal data shall be obtained only for one or more specified and lawful purposes;
3. Personal data shall be adequate, relevant and not excessive;
4. Personal data shall be accurate and, where necessary, kept up to date;
5. Personal data processed for any purpose shall not be kept for longer than is necessary for that purpose or those purposes;
6. Personal data shall be processed in accordance with the rights of individuals under the Data Protection Act 1998;
7. Personal data shall be kept secure i.e. protected by an appropriate degree of security;
8. Personal data shall not be transferred to a country or territory outside the European Economic Area, unless that country or territory ensures an adequate level of data protection.

Data Types

GDPR defines different types of data and prescribes how it should be treated.

Personal data

SSC will have access to a wide range of personal information and data. The data may be held in a digital format or on paper records. Personal data will include:

- → Personal information about members of SSC community – including clients, Employees and parents / carers e.g. names, addresses, contact details, legal guardianship contact details, disciplinary records
- → Curricular / academic / Social Care data - class lists, pupil / student progress records, reports, references
- → Professional records e.g. employment history, taxation and national insurance records, appraisal records, disciplinary records and references
- → Any other information that might be disclosed by parents / carers / Employees or by other agencies working with families or Employees.

Special Category Data

"Special Category Data" is more sensitive, and so needs more protection. In SSC the most likely special category data is likely to be:

- → Information on the racial or ethnic origin of a client or Employee
- → Information about the sexuality of a child, their family or an Employee
- → Medical & Social Care information about a child or Employee (SEND)
- → Some information regarding safeguarding will also fall into this category

Other types of Data not covered by the act

This is data that does not identify a living individual and could include Lesson Plans & key working sessions (where no individual pupil is named), Teaching & Care Resources, and other information about SSC which does not relate to an individual. Some of this data would be available publicly (for instance the diary of events for the forthcoming year).

Commitment

SSC is committed to effective management of Data Protection and maintaining the above principles at all times. Therefore, we will:

- → Appoint a Data Protection Officer to manage data
- → Inform individuals why personal information is being collected.
- → Inform individuals when their information is shared, and why and with whom unless the Data Protection Act provides a reason not to do this.
- → Check the accuracy of the information it holds and review it at regular intervals.
- → Ensure that only authorised personnel have access to the personal information whatever medium (paper or electronic) it is stored in.

- → Ensure that clear and robust safeguards are in place to ensure personal information is kept securely and to protect personal information from loss, theft and unauthorised disclosure, irrespective of the format in which it is recorded.
- → Ensure that personal information is not retained longer than it is needed.
- → Ensure that, when information is destroyed, it is done so appropriately and securely.
- → Share personal information with others only when it is legally appropriate to do so.
- → Comply with the duty to respond to requests for access to personal information, known as

Subject Access Requests

- → Ensure that personal information is not transferred outside the EEA without the appropriate safeguards.
- → Ensure all employees are aware of, and understand, these policies and procedures.
- → Ensure all employees complete GDPR online training relating to their specific job role.

Risk Management – Data Protection Officer (DPO)

The role of the DPO will include:

- → To inform and advise the organisation and its employees about their obligation to comply with the GDPR and other data protection laws
- → To monitor compliance with the GDPR and other data protection laws, including managing internal data protection activities, advise on data protection impact assessments; train employees and conduct internal audits
- → To be the first point of contact for supervisory authorities and for individuals whose data is processed (employees, customers etc.)

Risk Management – Employee and Directors Responsibilities

- → Everyone in SSC has the responsibility of handling personal information in a safe and secure manner.
- → Directors are required to comply fully with this policy in the event that they have access to personal data, when engaged in their role as a Director.

Retention of Personal Data

1. SSC shall not keep personal data for any longer than is necessary in light of the purpose or purposes for which that personal data was originally collected, held, and processed.
2. Different types of personal data, used for different purposes, will necessarily be retained for different periods and its retention periodically reviewed.
3. When establishing and/or reviewing retention periods, the following shall be taken into account:
    i. The type of personal data in question;
    ii. The purpose(s) for which the data in question is collected, held, and processed;
    iii. The Services legal basis for collecting, holding, and processing that data;
    iv. The category or categories of data subject to whom the data relates;
    v. The retention periods stipulated by Ofsted.
4. If a precise retention period cannot be fixed for a particular type of data, criteria shall be established by which the retention of the data will be determined, thereby ensuring that the data in question, and the retention of that data, can be regularly reviewed against those criteria.
5. In addition, the following defined retention periods, certain personal data may be deleted or otherwise disposed of prior to the expiry of its defined retention period where a decision is made within the Service to do so (whether in response to a request by a data subject or otherwise).
6. We will specify the retention period of personal data records and carry out disposal of data which exceed the retention period in accordance with data protection. When any personal data has served its purpose, it will be disposed of accordingly.
7. In limited circumstances, it may also be necessary to retain personal data for longer periods where such retention is required by Ofsted, or other regulators or in the public interest. All such retention will be subject to the implementation of appropriate technical and organisational measures to protect the rights and freedoms of data subjects, as required by the GDPR.

8. As per Children's Homes (England) Regulations 2015, Regulation 36, in relation to the retention of Children's case records for children accommodated in children's homes. These documents will be retained for either:
   Until the 75th anniversary of the child's birth,
   Or
   If the child dies before age 18, for 15 years from the date of death.

Transporting, Storing and Disposing of Personal Data

SSC will ensure that ICT systems are set up so that the existence of protected files is hidden from unauthorised users and that users will be assigned a clearance that will determine which files are accessible to them. Access to protected data will be controlled according to the role of the user. Employees will not, as a matter of course, be granted access to the whole management information system.

Storage and Access to Data - Technical Requirements

- → Personal data may only be accessed on machines that are securely password protected. Any device that can be used to access data must be locked if left unattended (even for very short periods).
- → All storage media must be stored in an appropriately secure and safe environment that avoids physical risk, loss or electronic degradation.
- → Personal data can only be stored on SSC equipment (this includes computers and portable storage media (where allowed). Private equipment (i.e. owned by the users) must not be used for the storage of personal data.
- → SSC has clear policy and procedures for the automatic backing up, accessing and restoring all data held on SSC systems, including off-site backups.

Portable Devices

When personal data is stored on any portable computer system:

- → The data must be encrypted and password protected.
- → The device must be password protected.
- → The data must be securely deleted from the device, in line with school policy once it has been transferred or its use is complete.
- → Data storage of personal information on removal media e.g. USB, portable hard drive, is not allowed, even if encrypted.
- → Employees may only use removable media e.g. USB, portable hard drive to transfer non personal information
- → All users will use strong passwords which must be changed regularly. User passwords must never be shared.

Images

- → Images of clients will only be processed and transported by use of authorised agents of SSC and permission for this will be obtained in the privacy notice or other photographic permission notice.
- → Images will be protected and stored in a secure area.

Cloud Based Storage

SSC has clear policy and procedures for the use of "Cloud Based Storage Systems" and is aware that data held in remote and cloud storage is still required to be protected in line with the Data Protection Act. SSC will ensure that it is satisfied with controls put in place by remote / cloud-based data services providers to protect the data.

Third Party Data Transfers

As a Data Controller, SSC is responsible for the security of any data passed to a "third party". Data Protections clauses will be included in all contracts where data is likely to be passed to a third party as well as data processing agreements.

Retention of Data

→ The guidelines given by the insurers will be used to determine how long data is retained.
→ Personal data that is no longer required will be destroyed and this process will be recorded. Persuading Employees to reduce the quantity of personal information they have collected over time should be regarded as an important priority.

Systems to Protect Data

Paper Based Systems

→ All paper based personal data will be protected by appropriate controls.
→ Paper based personal information sent to parents will be checked before the envelope is sealed.

Websites

→ Uploads to SSC website will be checked prior to publication.

E-mail

→ Where technically possible, all e-mails containing sensitive information must be encrypted.
→ The use of a secure e-mail system allows for secure communication.

Data Breach – Procedures

In the event of a data breach the data protection officer will inform the Registered Manager and the Directors

All Data Breaches will be handled in accordance with the ICO guidelines.

Policy Review Reviewing:

This policy will be reviewed and updated, if necessary, every two years or when legislation changes.

Right to Erasure (The "Right to Be Forgotten")

GDPR includes a right to erasure – but this is not an absolute right and does not necessarily override the lawful basis for continuing to hold data. This does not mean the data will never be erased. It will still not be retained for any longer than necessary, in accordance with statutory requirements and/or SSC's data retention guidelines.

1. Data subjects are entitled to require a controller to delete their personal data if the continued processing of those data is not justified
    i. The Data Protection Officer and controller for Stepping Stones is:
    Gurpreet Singh, Director – gurpreet@steppingstonescare.com
2. Data subjects have the right to erasure of personal data (the "Right to be Forgotten") if:
    i. The data are no longer needed for their original purpose (and no new lawful purpose exists);
    ii. The lawful basis for the processing is the data subject's consent, the data subject withdraws that consent, and no other lawful ground exists;
    iii. The data subject exercises the right to object, and the controller has no overriding grounds for continuing the processing;
    iv. The data have been processed unlawfully; or
    v. Erasure is necessary for compliance with EU law or the National Law of the relevant Member State.
    vi. In the event that any personal data that is to be erased in response to a data subject's request has been disclosed to third parties, those parties shall be informed of the erasure (unless it is impossible or would require disproportionate effort to do so).

Disposal of Personal Data

When any personal data is to be erased or otherwise disposed of for any reason (including where copies have been made and are no longer needed), it should be securely deleted and disposed of.

Complaints

Complaints will be dealt with in accordance with the SSC Complaints Policy. Complaints relating to the handling of personal information may be referred to the Information Commissioner.

Review

This policy will be reviewed as it is deemed appropriate, but no less frequently than every year. The policy review will be undertaken by the Responsible Individual or nominated representative.