Information Security
Data Exchange Agreement
2024 - 2026

Author:	*Data Protection Officer*
Owner:	*Data Protection Officer*
3rd Party:	*<3rd party>*
Reference:	*2022/DEA/SMAT*
Date:	*1st December 2024*
Version:	*1*
Status:	*Final*

Table of Contents

1 Overview

In making this agreement due attention has been paid to the relevant legislation where applicable, including:

- The Data Protection Act 2018 (DPA)
- The General Data Protection Regulation 2018 (GDPR)
- The Freedom of Information Act 2000 (FOI)

According to the Data Protection Act, any organisation which determines the purposes for which and manner in which any personal data are, or are to be, processed is a "data controller". All data controllers are required to comply with the DPA whenever they process personal data (bearing in mind, as stated above, that "processing" includes collecting, storing, amending, and disclosing data). At all times, when sharing data with other organisations, the organisation responsible for collecting, presenting, and exchanging the data shall be considered as a data controller. Organisations which receive data from that responsible delivery authority are considered to be "data processors" until such time as they undertake processing activities towards their own objectives. By this definition, the parties to this agreement will be considered a controller of the data exchanged.

This agreement defines how all data including personal and special category data will be shared between the data controllers, and the methods used for the secure and legal transmission, storage, and processing of that data.

1.1 Purpose of this Data Exchange Agreement

This agreement is made to allow the parties to share personal data about students and former students to support the effective safeguarding of children and young people, meet the needs of students in examinations and assessments (through the sharing of agreed access arrangements and the assessments to support these), fulfil the statutory duties of schools and colleges to support the tracking of participation in post-16 education, and to allow schools to measure the impact of their provision through post-18 destinations. The parties will therefore exchange personal data on the legal basis of public task and have informed data subjects of this transfer through the provisions of Seva School and 3rd Party Privacy Notices and communications.

1.2 The Data Controllers

Seva School incorporated under the Further and Higher Education Act 1992. The school is registered with the Office of the Information Commissioner as a data controller, registration number Z4617228. The school provides education and skills to young people, and stores a range of personal and special category data to support claims for funding, education tracking and administration and the management of the business.

Seva School is registered with the Office of the Information Commissioner as a -data controller. The organisation provides secondary education and stores a range of personal and special category data to support claims for funding, education and sporting activity tracking and administration and the management of the organisation.

In respect of the data provided by one party to the other, the receiving party shall act as a data controller in their use of the data from the point of receipt. All input data, information produced during processing, and final outputs will be treated as confidential and or sensitive and used only for the purposes outlined in this agreement unless specific consent has been obtained from the data subject.

2 Types of Data

For the purposes of this agreement there are four classes of data as listed below:

2.1 Anonymised and Aggregated Data

Anonymised data are individual data records from which the personally identifiable fields have been removed. It should be noted that where the receiving party removes name and address information, fields such as date-of-birth, post code and qualifications may not be removed, due to the nature of activities undertaken, but such data will still be "anonymised" ensuring that the data subject's identity is not discernible from such data.

Aggregated data are data which are processed to produce a generalised result, and from which individuals cannot be identified. This might include data brought together to give a broad understanding of e.g., ethnicity distribution. There is sometimes a slight risk that aggregated data might still allow an individual to be identified, for example by the results producing a very small group of results, from which other data may be used in identifying an individual, even though personal data has been removed. The parties to this agreement shall take all reasonable steps to ensure that such cases are identified and resolved before any aggregated data is shared.

2.2 Personal Data

In the Data Protection Act personal data are defined as data which relate to a living individual who can be identified from those data, or from those data and other information which is in the possession of, or is likely to come into the possession of, the data controller, and includes any 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.

Such personal data might include, but is not limited to:

- Name , Address, Telephone Number
- Date of Birth / Age,
- Application or course history
- A unique reference number if that number can be linked to other information which identifies the data subject.

The law imposes obligations and restrictions on the way the Data Controller and its partners process personal data (in this context processing includes collecting, storing, amending and disclosing data), and the individual who is the subject of the data, the "data subject" has the right to know who holds their data and how such data are or will be processed, including how such data are to be shared.

2.3 Business Data

In the context of this agreement, Business Data is defined as data relating to a limited company or public body, including the details of owners, directors, and employees. Such data, when referencing an individual, continues to meet the definition of personal data according to UK Data Protection Law, and therefore subject to the controls set out within this agreement.

The law imposes the same obligations and restrictions on the way the Data Controller and its partners process personal data (in this context processing includes collecting, storing, amending and disclosing data), and the individual who is the subject of the data, the "data subject" has the right to know who holds their data and how such data are or will be processed, including how such data are to be shared.

2.4 Sensitive Data

In the Data Protection Act certain types of data are referred to as "special category data". These are data which relate to the data subject's:

- Racial or ethnic origin
- Political opinions
- Religious beliefs, or other beliefs of a similar nature
- Trade union membership
- Physical or mental health or condition
- Sexual life
- Commission or alleged commission of any offence
- Any proceedings for any offence committed or alleged to have been committed.

Additional and more stringent obligations and restrictions apply to the control and processing of sensitive personal data. Any agreement to exchange sensitive data will be subject to a Data Protection Impact Assessment completed by the sharing Data Controller, as required by Seva School Data Protection Policy.

3 Data Management

3.1 Use of Personal Data

All parties shall ensure that data exchanged within the scope of this agreement is only used for the purposes for which it was exchanged.

3.2 Controls

It is recognised that the receiving data controller may be required to report on and summarise data including personal and special category data. The receiving data controller therefore agrees to treat all datasets containing any information about individuals with the same care and privacy, and in particular:

- Ensure that all outputs, reports, and summaries produced from the data are checked to ensure that individual identity and confidentiality is protected; or to mark all outputs appropriately detailing the personal and/or sensitive data they contain and the intended audience.
- Take reasonable steps to protect personal data from unauthorised modification or changes which result in the data becoming inaccurate or incomplete.
- Take all reasonable steps to ensure the security of data during processing.
- Delete all data and associated analysis upon completion of agreed activities, accepting that some data may have been used to update or create data then controlled by them.

4 Data Control

4.1 Data Protection Registration

All organisations that manage, access, process and share personal data must be registered with the Information Commissioner's Office (ICO). The data controller(s) named in this agreement are registered with the ICO and are responsible for registering all required classes of information prior to collection or processing.

4.2 Privacy Notices and Public Information

Each party will ensure that Privacy Notices and Public Information in respect of data protection is complete, up to date, and makes appropriate reference to the parties and terms of this agreement and is responsible for ensuring that data subjects are aware of the planned sharing and processing activities.

4.3 Indemnity

Each party will keep each of the other parties indemnified against any and all costs, expenses and claims arising out of any breach of this agreement and in particular, but without limitation, the unauthorised or unlawful access, loss, theft, use, destruction or disclosure by the offending organisation or its sub-contractors, employees, agents or any other person within the control of the offending organisation of any data obtained in connection with this agreement.

5 Security

5.1 Sharing of Data

All data shared under this agreement will be encrypted and password protected prior to transport from or on return to the originating data controller. All reasonable steps will be taken to protect the security of the data including;

- Password protected encryption using unique passwords for each file for each movement
- Use of secure file storage where possible to provide 2 factor protection over the data
- Use of encrypted e-mail only where secure file stores cannot be accessed
- **No** use of physical media such as memory sticks or CDs/DVDs to transport data
- Separation of encrypted files through use of different transport media

All data exchange will be facilitated through named contacts for the two organisations:

-Mr Ben Sturmey (Careers Lead) and Mrs Kulbir Convery (Careers co-ordinator) for Seva School

-The 3rd Party

Named contacts shall take responsibility for the encryption and transport of data, including appropriate checks and reporting of any data loss or breach of security arrangements.

5.2 Storage of Data

Data provided for processing will be stored with appropriate password protection in a secure location. This storage will be protected by standard Active Directory security in addition to the file level protection applied.

Where local storage is used, for example during the processing of a file, all data will be held on a secure encrypted hard disc drive with the same password protections.

5.3 Confidentiality of Data

All personal data is treated with the utmost confidentiality and will not be shared with any third party. All such 3rd party requests for access to detailed or summary data shall be referred to the originating data controller for consideration.

Any agreed sharing of summary, non-personal data shall be subject to separate agreement between all parties.

Data which falls within this agreement must be anonymised if used for training purposes.

Any breach of security or confidentiality shall be managed by the appropriate data controller and reported to the originating data controller immediately. All reasonable assistance will be given by both parties to identify the cause and nature of the breach and any impact on the organisations and/or any individual.

6 Requests about Personal Data held.

6.1 Subject Access Requests

The parties to this agreement, as controllers of the data processed by them, will be responsible for all subject access requests. Data subjects will be aware of the exchange of data under this agreement allowing them to make distinct requests of each party as required.

6.2 Complaints

Complaints about Personal Data held by a data controller must be made in writing to the person or organisation holding this information, detailing the reasons for the complaint. Complaints regarding the accuracy of data shared under this agreement should be made in writing, shared with all parties to allow for corrections to be agreed, and should be responded to within 14 days.

7 Changes to Agreements

7.1 Periodic Changes

This agreement will be reviewed periodically and consequently it may be subject to change.

7.2 Breaches of Confidentiality or Security

Where a breach of confidentiality or security of data exchanged occurs, or a risk is identified which may cause a breach, the matter will first be investigated and reported on by the data controller. During any such investigation, this agreement may be suspended by either party, and will be reviewed upon completion of the investigation.

7.3 Termination

This agreement will terminate on the 31st of August following the agreement date, and must be renewed annually thereafter.

In addition, either party may terminate this agreement with immediate effect in the event of a breach of confidentiality or security, or if there are concerns of a material risk of a data breach. In the event of either party terminating the agreement early, the reasons for termination will be clearly outlined to the other party, and the organisation's usual process for complaint handling will apply.

For <3rd Party>

Signed: _____

Name:

(block capitals) _____ Date _____

For Seva School

Signed: B Sturmey

Name: BEN STURMEY

(block capitals) Date 1/12/2024