Data Protection and Handling Policy

Introduction

This policy sets out OTT SCITT's (or the "SCITT") commitment to the lawful and fair handling of personal data in accordance with the UK General Data Protection Regulation (UK GDPR) and the Data Protection Act 2018. The Data Protection Act 2018 ("the Act") regulates the holding and processing of personal data - that is information relating to living individuals, which is held either in paper or electronic form. The Act also gives rights to individuals whose personal information is held by organisations.

The SCITT needs to collect and use personal information in order to carry out its functions effectively. Information can be held concerning its current, past and prospective Associate Teachers, employees, suppliers, service users, and others with whom the Trust communicates. The SCITT and in some circumstances its individual employees could face prosecution for failure to handle personal data in accordance with the Act.

1. Definitions

Term	Definition
Personal data	Any information relating to an identified, or identifiable, individual. This may include the individual's: • Name including surname • Identification number • Location data • Online identifier, such as a username It may also include factors specific to the individual's physical, physiological, genetic, mental, economic, cultural or social identity
Special categories of personal data	Personal data which is more sensitive and so needs more protection, including information about an individual's: • Racial or ethnic origin • Political opinions • Religious or philosophical beliefs • Trade union membership • Genetics • Biometrics (such as fingerprints, retina and iris patterns), where used for identification purposes • Health – physical or mental • Sex life or sexual orientation
Processing	Anything done to personal data, such as collecting, recording, organising, structuring, storing, adapting, altering, retrieving, using, disseminating, erasing or destroying. Processing can be automated or manual.
Data subject	The identified or identifiable individual whose personal data is held or processed.

Data controller	A person or organisation that determines the purposes and the means of processing of personal data: in this case, the data controller is the SCITT
Data processor	A person or other body, other than an employee of the data controller, who processes personal data on behalf of the data controller.
Personal data breach	A breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data.

2. Roles and Responsibilities

This policy applies to all staff employed by Oxfordshire Teacher Training, and to external organisations or individuals working on our behalf, including Associate Teachers, Mentors, Senior Links, Visiting Tutors and Subject Specialists.

2.1 Governing board

The governing board has overall responsibility for ensuring that our school complies with all relevant data protection obligations.

3.2 Data protection officer

The data protection officer (DPO) is responsible for overseeing the implementation of this policy, monitoring our compliance with data protection law, and developing related policies and guidelines where applicable. They will provide an annual report of their activities directly to the governing board and, where relevant, report to the board their advice and recommendations on SCITT data protection issues. The DPO is also the first point of contact for individuals whose data the SCITT processes, and for the ICO.

The DPO for The SCITT is Matthew Coatsworth (matthew.coatsworth@ott-scitt.org.uk).

3.3 SCITT Manager

The SCITT Manager acts as the representative of the data controller on a day-to-day basis.

3.4 Central SCITT team, Associate Teachers, Visiting Tutors, Subject Specialists, Mentors and Senior Links

Staff are responsible for:

- Collecting, storing and processing any relevant personal data or special categories of personal data in accordance with this policy
- Informing the SCITT of any changes to their personal data
- Contacting the DPO in the following circumstances:
    - With any questions about the operation of this policy, data protection law, retaining personal data or keeping personal data secure
    - If they have any concerns that this policy is not being followed
    - If they are unsure whether or not they have a lawful basis to use personal data in a particular way
    - If they need to rely on or capture consent, draft a privacy notice, deal with data protection rights invoked by an individual, or transfer personal data outside the European Economic Area
    - If there has been a data breach
    - Whenever they are engaging in a new activity that may affect the privacy rights of individuals
    - If they need help with any contracts or sharing personal data with third parties

4. Policy Statement

Any personal data which the SCITT collects, records or uses in any way whether it is held on paper, computer or other media will be subject to appropriate safeguards to ensure that the SCITT complies with the Act.

The SCITT fully endorses and adheres to the eight Data Protection Principles which are set out in the Act and summarised below. Personal data shall be:

1. Processed fairly and lawfully and in a transparent way;
2. Collected for specified, explicit and legitimate purposes and not in any way which would be incompatible with those purposes
3. Adequate, relevant and limited to what is necessary to fulfil the purposes for which it is processed;
4. Accurate and, where necessary, kept up to date;
5. Not kept for longer than is necessary for the purposes for which it is processed;
6. Processed in line with the data subject's rights;
7. Processed in a way that ensures it is appropriately secure ;
8. Not transferred to a country which does not have adequate data protection laws.

Lawfulness, fairness and transparency

We will only process personal data where we have one of six 'lawful bases' (legal reasons) to do so under data protection law:

- The data needs to be processed so that the SCITT can **fulfil a contract** with the individual, or the individual has asked the school to take specific steps before entering into a contract
- The data needs to be processed so that the SCITT can **comply with a legal obligation**
- The data needs to be processed to ensure the **vital interests** of the individual e.g. to protect someone's life
- The data needs to be processed so that the SCITT, as a public authority, can perform a task **in the public interest,** and carry out its official functions
- The data needs to be processed for the **legitimate interests** of the SCITT or a third party (provided the individual's rights and freedoms are not overridden)
- The individual (or their parent/carer when appropriate in the case of a pupil) has freely given clear **consent**

For special categories of personal data, we will also meet one of the special category conditions for processing which are set out in the UK GDPR and Data Protection Act 2018.

5. Action

In order to meet the requirements of the data protection principles and its obligations under the Act, the SCITT will ensure the following:

1. Ensure the River Learning Trust renews entry of the Register of Notifications held by the Information Commissioner's Office;
2. Maintain a register of particulars about the types of personal data the SCITT holds, purposes for which it is held and used and types of organisations to which personal data may be disclosed;
3. Appoint officers with specific responsibility for data protection in the SCITT;
4. Any forms used to collect data will contain a 'fair processing notice' to inform the data subject of the reasons for collecting the personal information and the intended uses;
5. Any personal information that has been collected will be used only for the purposes for which it was collected;
6. Data subjects (individuals to whom the personal information relates) are able to exercise their rights under the Act, including the right:
    - to be informed that their personal information is being processed
    - of access to their personal information
    - to correct, rectify, block or erase information that is regarded as wrong
7. Personal data will only be disclosed to third parties when it is fair and lawful to do so in accordance with the Act and with any Information Sharing Protocols;

8. Sensitive personal data will only be processed with the explicit consent of the data subject or if an exemption applies under the Act. Sensitive data is personal data about an individual's racial or ethnic origin, political opinions, religious beliefs, trade union membership, physical or mental health, sex life, details of the commission or alleged commission of any offence and any court proceedings relating to the commission of an offence;
9. Procedures are in place to check the accuracy of personal data collected, retained and disclosed;
10. Review the time that personal information is retained or stored to ensure that it is erased at the appropriate time;
11. Compliance with the Code of Good Practice set out in ISO 17799 which sets out the requirements for an Information Security Management System;
12. All officers who hold or process personal information will receive appropriate training in order to comply with the Act, and
13. Audit compliance with this policy and the Act and any incidents involving breaches of this policy or the Act are recorded, analysed and disciplinary action taken as appropriate.

This policy is reviewed every two years or sooner if there is a change in legislation.

APPENDIX A
Privacy Information and rights for individuals
Privacy Information

Individuals have the right to be informed about the collection and use of their personal data.

The SCITT provides individuals with privacy information including:

- Purposes for processing their personal data
- Retention periods for that personal data
- Who it will be shared with

The SCITT will provide privacy information to individuals at the time personal data is collected. If personal data is obtained from other sources, the SCITT will provide privacy information within a reasonable period of obtaining the data and no later than one month.

Individuals also have the right to access personal data and supplementary information. Where a request for access has been made, details are stored on the SCITT *Subject Access Request* file. For more details, see the SCITT *Data Protection Procedures* document.

The GDPR includes a right for individuals to have inaccurate personal data rectified, or completed if it is incomplete. An individual can make a request for rectification verbally or in writing. The SCITT will respond within one calendar month, although in certain circumstances it may refuse the request if manifestly unfounded or excessive. In these instances, justification will be given.

Under Article 17 of the GDPR individuals have the right to have personal data erased. This is also known as the 'right to be forgotten'. The right is not absolute and only applies in certain circumstances. Where applicable, the SCITT will respond within one month of receipt.

Additional rights include:

- The right to restrict processing
- The right to data portability

- The right to object
- Rights in relation to automated decision making and profiling

Where applicable, the SCITT will respond within one month of receipt.

Sharing personal data
We will not normally share personal data with anyone else, but may do so where:

- There is an issue that puts the safety of our staff at risk
- We need to liaise with other agencies – we will seek consent as necessary before doing this
- Our suppliers or contractors need data to enable us to provide services to our staff – for example, IT companies. When doing this, we will:
    - Only appoint suppliers or contractors which can provide sufficient guarantees that they comply with data protection law
    - Establish a data sharing agreement with the supplier or contractor, either in the contract or as a standalone agreement, to ensure the fair and lawful processing of any personal data we share
    - Only share data that the supplier or contractor needs to carry out their service, and information necessary to keep them safe while working with us

We will also share personal data with law enforcement and government bodies where we are legally required to do so, including for:

- The prevention or detection of crime and/or fraud
- The apprehension or prosecution of offenders
- The assessment or collection of tax owed to HMRC
- In connection with legal proceedings
- Where the disclosure is required to satisfy our safeguarding obligations
- Research and statistical purposes, as long as personal data is sufficiently anonymised or consent has been provided

We may also share personal data with emergency services and local authorities to help them to respond to an emergency situation that affects any pupils or staff.
Where we transfer personal data to a country or territory outside the European Economic Area, we will do so in accordance with data protection law.

Storage, Handling and Access
Electronic Storage
In accordance with legislation, the SCITT will ensure that all collected personal information is recorded electronically in folders with monitored and restricted access, and within password protected documents as appropriate. All forms used to collect data include disclaimers and are listed in the SCITT's *Data Protection Procedures* document. All electronic databases in use are also listed, along with users who can access them, in the *Data Protection Procedures* document. These databases are secured by individual usernames and passwords.

Handling of Paper Documents
Any documents required in paper form should be kept securely, in lockable, non-portable, storage containers with access strictly controlled and limited to those who are entitled to see it as part of their duties. The SCITT will also ensure that offices containing folders with any personal information remain monitored and locked, with code locking systems fitted and entrance restricted to only those who require access. The SCITT will ensure that information is only passed on to those who are authorised to receive it in the course of their duties. For more details, see *Data Protection Procedures* document.

Access

Where we need to share personal data with a third party, we carry out due diligence and take reasonable steps to ensure it is stored securely and adequately protected.

Individuals have a right to make a 'subject access request' to gain access to personal information that the SCITT holds about them. This includes:

- Confirmation that their personal data is being processed
- Access to a copy of the data
- The purposes of the data processing
- The categories of personal data concerned
- Who the data has been, or will be, shared with
- How long the data will be stored for, or if this isn't possible, the criteria used to determine this period
- The source of the data, if not the individual
- Whether any automated decision-making is being applied to their data, and what the significance and consequences of this might be for the individual

Subject access requests must be submitted in writing, either by letter or email to the DPO. They should include:

- Name of individual
- Correspondence address
- Contact number and email address
- Details of the information requested

If staff receive a subject access request they must immediately forward it to the DPO.

Responding to subject access requests

When responding to requests, we:

- May ask the individual to provide 2 forms of identification
- May contact the individual via phone to confirm the request was made
- Will respond without delay and within 1 month of receipt of the request
- Will provide the information free of charge
- May tell the individual we will comply within 3 months of receipt of the request, where a request is complex or numerous. We will inform the individual of this within 1 month, and explain why the extension is necessary

We will not disclose information if it:

- Might cause serious harm to the physical or mental health of a pupil or another individual
- Would reveal that a child is at risk of abuse, where the disclosure of that information would not be in the child's best interests
- Is contained in adoption or parental order records
- Is given to a court in proceedings concerning a child

If the request is unfounded or excessive, we may refuse to act on it, or charge a reasonable fee which takes into account administrative costs. A request will be deemed to be unfounded or excessive if it is repetitive, or asks for further copies of the same information. When we refuse a request, we will tell the individual why, and tell them they have the right to complain to the ICO.

Other data protection rights of the individual

In addition to the right to make a subject access request (see above), and to receive information when we are collecting their data about how we use and process it, individuals also have the right to:

- Withdraw their consent to processing at any time

- Ask us to rectify, erase or restrict processing of their personal data, or object to the processing of it (in certain circumstances)
- Prevent use of their personal data for direct marketing
- Challenge processing which has been justified on the basis of public interest
- Request a copy of agreements under which their personal data is transferred outside of the European Economic Area
- Object to decisions based solely on automated decision making or profiling (decisions taken with no human involvement, that might negatively affect them)
- Prevent processing that is likely to cause damage or distress
- Be notified of a data breach in certain circumstances
- Make a complaint to the ICO
- Ask for their personal data to be transferred to a third party in a structured, commonly used and machine-readable format (in certain circumstances)

Individuals should submit any request to exercise these rights to the DPO. If staff receive such a request, they must immediately forward it to the DPO.

Retention

Once a recruitment (or other relevant) decision has been made, the SCITT does not keep personal information for any longer than is necessary. Throughout this time, the conditions regarding the safe storage and controlled access will prevail. For more details, see *Data Protection Procedures* document.

Disposal

Once the retention period has elapsed, the SCITT processors will ensure that any information is immediately destroyed by secure means, for example by shredding, pulping or burning. While awaiting destruction, certificate information will not be kept in any insecure receptacle (e.g. waste bin or confidential waste sack).

Data Protection by Design and Default

We will put measures in place to show that we have integrated data protection into all of our data processing activities, including:

- Appointing a suitably qualified DPO, and ensuring they have the necessary resources to fulfil their duties and maintain their expert knowledge
- Only processing personal data that is necessary for each specific purpose of processing, and always in line with the data protection principles set out in relevant data protection law (see section 6)
- Completing privacy impact assessments where the school's processing of personal data presents a high risk to rights and freedoms of individuals, and when introducing new technologies (the DPO will advise on this process)
- Integrating data protection into internal documents including this policy, any related policies and privacy notices
- Regularly training members of staff on data protection law, this policy, any related policies and any other data protection matters; we will also keep a record of attendance
- Regularly conducting reviews and audits to test our privacy measures and make sure we are compliant
- Maintaining records of our processing activities, including:
    - For the benefit of data subjects, making available the name and contact details of our school and DPO and all information we are required to share about how we use and process their personal data (via our privacy notices)
    - For all personal data that we hold, maintaining an internal record of the type of data, data subject, how and why we are using the data, any third-party recipients, how and why we are storing the data, retention periods and how we are keeping the data secure

Personal data breaches
The SCITT will make all reasonable endeavours to ensure that there are no personal data breaches. In the unlikely event of a suspected data breach, we will follow the procedure set out in appendix 1.

When appropriate, we will report the data breach to the ICO within 72 hours. Such breaches in a SCITT context may include, but are not limited to:

- Safeguarding information being made available to an unauthorised person
- The theft of a laptop containing non-encrypted personal data about Associate Teachers
- A non-anonymised dataset being published on the SCITT website which shows personal data about Associate Teachers

Training
All staff and governors are provided with data protection training as part of their induction process. Data protection will also form part of continuing professional development, where changes to legislation, guidance or the school's processes make it necessary.

Person responsible for policy: SCITT Director
Reviewed October 2022
To be reviewed October 2024 or earlier

Please also refer to other related documents: *DBS Handling; Safer Recruitment; River Learning Trust Data Protection Policy, SCITT Data Protection Procedures, SCITT Subject Access Request*

Appendix B
Personal data breach procedure

This procedure is based on guidance on personal data breaches produced by the ICO.

- On finding or causing a breach, or potential breach, the staff member or data processor must immediately notify the DPO
- The DPO will investigate the report, and determine whether a breach has occurred. To decide, the DPO will consider whether personal data has been accidentally or unlawfully:
    - Lost
    - Stolen
    - Destroyed
    - Altered
    - Disclosed or made available where it should not have been
    - Made available to unauthorised people
- The DPO will alert the Director of the SCITT, the Chief Executive of the River Learning Trust and the chair of governors
- The DPO will make all reasonable efforts to contain and minimise the impact of the breach, assisted by relevant staff members or data processors where necessary. (Actions relevant to specific data types are set out at the end of this procedure)
- The DPO will assess the potential consequences, based on how serious they are, and how likely they are to happen
- The DPO will work out whether the breach must be reported to the ICO. This must be judged on a case-by-case basis. To decide, the DPO will consider whether the breach is likely to negatively affect

people's rights and freedoms, and cause them any physical, material or non-material damage (e.g. emotional distress), including through:
    - Loss of control over their data
    - Discrimination
    - Identify theft or fraud
    - Financial loss
    - Unauthorised reversal of pseudonymisation (for example, key-coding)
    - Damage to reputation
    - Loss of confidentiality
    - Any other significant economic or social disadvantage to the individual(s) concerned

  If it is likely that there will be a risk to people's rights and freedoms, the DPO must notify the ICO.
- The DPO will document the decision (either way), in case it is challenged at a later date by the ICO or an individual affected by the breach. Documented decisions are stored on The Cherwell School Network Central SCITT section

- Where the ICO must be notified, the DPO will do this via the 'report a breach' page of the ICO website within 72 hours. As required, the DPO will set out:
    - A description of the nature of the personal data breach including, where possible:
        - The categories and approximate number of individuals concerned
        - The categories and approximate number of personal data records concerned
    - The name and contact details of the DPO
    - A description of the likely consequences of the personal data breach
    - A description of the measures that have been, or will be taken, to deal with the breach and mitigate any possible adverse effects on the individual(s) concerned
- If all the above details are not yet known, the DPO will report as much as they can within 72 hours. The report will explain that there is a delay, the reasons why, and when the DPO expects to have further information. The DPO will submit the remaining information as soon as possible
- The DPO will also assess the risk to individuals, again based on the severity and likelihood of potential or actual impact. If the risk is high, the DPO will promptly inform, in writing, all individuals whose personal data has been breached. This notification will set out:
    - The name and contact details of the DPO
    - A description of the likely consequences of the personal data breach
    - A description of the measures that have been, or will be, taken to deal with the data breach and mitigate any possible adverse effects on the individual(s) concerned
- The DPO will notify any relevant third parties who can help mitigate the loss to individuals – for example, the police, insurers, banks or credit card companies
- The DPO will document each breach, irrespective of whether it is reported to the ICO. For each breach, this record will include the:
    - Facts and cause
    - Effects
    - Action taken to contain it and ensure it does not happen again (such as establishing more robust processes or providing further training for individuals)
- Records of all breaches will be stored The Cherwell School Network Central SCITT section
- The DPO and Director will meet to review what happened and how it can be stopped from happening again. This meeting will happen as soon as reasonably possible

Actions to minimise the impact of data breaches

We will take actions to mitigate the impact of different types of data breach, focusing especially on breaches involving particularly risky or sensitive information. We will review the effectiveness of these actions and amend them as necessary after any data breach.