

Overseas Transfers & Hosting



Title	Overseas Transfers & Hosting
Status	Approved
Version	2
Date Approved	03/05/2024
Review Date	02/05/2025

Contents

1. Introduction.....	2
2. Quick Reference Guide	2
3. Policy References.....	3
4. Procedures	3
4.1. Using Data Processors.....	3
4.2. Appropriate Safeguards.....	3
Adequacy Decisions	4
United States Data Privacy Framework (US-UK Data Bridge).....	4
International Data Transfer Agreements (IDTA)	5
International Data Transfer Addendum	5
An approved Code of Conduct.....	5
Certification under an approved certification scheme	5
Exceptions from the Safeguard requirements for Overseas Transfers	6
5. Record keeping	6
5.1. Privacy Notices.....	7
5.2. Records of Processing Activity	7
5.3. Risk Register	7
5.4. Processor Evidence Files	8
6. Advice and Support	8
7. Breach Statement.....	8
Annex A: Overseas Transfer Mechanisms.....	8

1. Introduction

When a Data Controller uses personal data, either itself or via a Data Processor, to deliver services which require handling personal data, the law makes clear that the Data Controller is still legally responsible for that data and that the Data Processor can only act on the Data Controller's instructions under a 'written contract'

It is important that if transfers of personal data are made to overseas countries, or you procure the services of a suppliers whose data centres and/or support services are located in an overseas country, that you comply with your legal obligation to ensure appropriate safeguards are in place to protect personal data. Data subjects must be assured that the same level of protection and the same rights will apply to the processing of their personal data overseas as it would if the data were processed in the UK.

The principle that the law introduces is this:

- If the Controller fails to have appropriate safeguards in place it is unlawful processing and therefore a personal data breach.
- Overseas transfers/hosting must be explained in your privacy notices and documented in your Records of Processing Activity and Data Protection Impact Assessments.
- Regulatory action (including monetary penalties) is taken against Controllers and also, where there is failure to follow instruction from Controllers, against Processors.

2. Quick Reference Guide

- All data transferred, stored or processed outside the UK must be identified and documented in your Records of Processing Activities (RoPA)
- Where an ad hoc transfer relates to student information, ensure you have consent from the Parent/Carer and where the child is twelve years of age or older, the child themselves. When gaining consent you must explain any risks to the personal data associated with the transfer to enable their consent to be informed
- Always record the informed consent and your rationale/justification for sending the personal data overseas
- When transfers relate to service provision e.g. Cloud services or systems, always ensure that you have a written contract with the supplier, or other agreement which is legally binding
- Where personal data will be transferred, received or stored in overseas countries without an adequacy decision ensure that, where the transfer is subject to a contractual arrangement, your contract includes the International Data Transfer Agreement

- Completing a Data Protection Impact Assessment will guide you to consider what assurances you need from any overseas supplier you wish to enter into a contract or agreement with
- Where data is being sent, held or supported from countries without an adequacy decision you must complete a [Transfer Risk Assessment](#) (TRA) before making the transfer
- Ensure you have documented which safeguards you will be relying on to support overseas transfers in your Privacy Notices and Records of Processing Activity.

3. Policy References

This procedure is a requirement of the Data Protection Policy.

4. Procedures

4.1. Using Data Processors

4.1.1 When procuring services you must always check if your processor is either based outside the UK or uses cloud services outside the UK. You will discover this through your DPIA process by using the supplier security questionnaire (SSQ).

4.1.2 Where they do, you must complete the TRA and apply an appropriate safeguard.

4.1.3 You, as data controller, are responsible for checking the location of processing by your processor. However, you must check with your processor if they use any sub-contractors. If they do, it is their responsibility to carry out a TRA for each sub-contractor. You must ask them to confirm that they have completed the TRAs and applied an appropriate safeguard. This can be achieved by using the SSQ.

4.2. Appropriate Safeguards

4.2.1. The first step is to establish a list of all the overseas organisations (and potentially some individuals) who you give (or allow them to access on your behalf) the personal data for which you are Data Controller. Once these data flows are identified you can assess which of the safeguards permitted by law apply for each flow.

4.2.2. The list of safeguards includes:

- a) An Adequacy Decision
- b) United States Data Privacy Framework (US-UK Data Bridge)
- c) International Data Transfer Agreement
- d) An ICO approved Code of Conduct

- e) An ICO approved Certification Scheme
- f) Exceptions to the Safeguards for Overseas Transfers

Adequacy Decisions

An adequacy decision is where an authorising body (in this case the ICO) accept an overseas countries evidence that they have in place the right laws to ensure that personal data processed in their country is subject to a sufficiently high level of protection, and that data subjects have the same rights as those in the UK. The ICO publish a list of countries with an adequacy decision, these currently include:

Countries in the European Union, and Iceland, Norway, Liechtenstein, Andorra, Argentina, Guernsey, Isle of Man, Israel, Jersey, New Zealand, Switzerland and Uruguay.

There are partial findings of adequacy about Japan and Canada.

- The adequacy finding for Japan only covers private sector organisations.
- The adequacy finding for Canada only covers data that is subject to Canada's Personal Information Protection and Electronic Documents Act (PIPEDA). Not all data is subject to PIPEDA.

You can view an up-to-date list of the countries which have an adequacy finding on the [ICO website](#). You should check back regularly for any changes.

United States Data Privacy Framework (US-UK Data Bridge)

The UK Extension to the EU-US Data Privacy Framework was developed to facilitate transatlantic commerce by providing US organisations with reliable mechanisms for personal data transfers to the United States from the United Kingdom, that are consistent with UK law. The US Data Bridge was effective October 12, 2023.

If you wish to make a transfer to, or use a supplier who processes personal data in, the US you should check the [DPF website](#) to check if recipient or supplier is registered.

To confirm whether an organisation is a DPF participant, go to the Data Privacy Framework List and search alphabetically or by typing in the organisation name in the search bar.

To confirm that the type of information to be transferred is covered by the organisation's DPF commitments click on the organisation's name within the [Data Privacy Framework List](#).

Within the organisation's DPF program record, review the "Other Covered US Entities and US Subsidiaries" section as well as the "Participation" section of the record.

To review the privacy policy that applies to the covered information, within the organisation's DPF program record, click on the link to the relevant privacy policy or policies (for HR data and/or non-HR data) under the "Privacy Policy" section of the record.

Registration to the Data Privacy Framework is equivalent to having an adequacy decision.

International Data Transfer Agreements (IDTA)

In March 2022 the [IDTA](#) replaced the current UK standard contractual clauses for international transfers outside the UK of personal data processed under the UK GDPR. They take into account the binding judgement of the European Court of Justice, in the case commonly referred to as "[Schrems II](#)". The agreement must be populated by the Data Controller but cannot be altered and must be used in full. Both parties must retain a copy of these clauses. The clauses can be added into an existing contract or included in a new contract.

These clauses provide legally binding responsibilities on parties to ensure that data subjects rights are protected when their personal data is processed in the recipient country and that they can seek legal redress for any unlawful processing. The clauses can only be relied on where the recipient country's domestic law supports data protection and does not have laws which entitle them to monitor or access personal data coming onto the country. These risks will be assessed as part of your TRA.

International Data Transfer Addendum

The Addendum can be added to the new EU Standard Contract Clauses to support data transfers as above, for personal data processed which is subject to both UK GDPR and EU GDPR. [This might apply for overseas students from the EU].

An approved Code of Conduct

You can make a restricted transfer, if the receiver has signed up to a code of conduct, which has been approved by us. The code of conduct must include appropriate safeguards to protect the rights of people whose personal data is transferred, with a binding and enforceable commitment by the receiver to apply those appropriate safeguards.

Certification under an approved certification scheme

You can make a restricted transfer if the receiver has a certification, under a scheme approved by the ICO. The certification scheme must include appropriate safeguards to protect the rights of people whose personal data is transferred, with a binding and enforceable commitment by the receiver to apply those appropriate safeguards.

Exceptions from the Safeguard requirements for Overseas Transfers

Where none of the above safeguards apply to the overseas transfer, and the transfer is **occasional** or a **one off**, you should consider whether an exception from the need for these safeguards is applicable. Those exceptions are:

a) **Explicit Consent**

As a valid consent must be both specific and informed, you must provide the individual with precise details about the restricted transfer. You cannot obtain a valid consent for restricted transfers in general.

You should tell the individual:

- the identity of the receiver, or the categories of receiver;
- the country or countries to which the data is to be transferred;
- why you need to make a restricted transfer;
- the type of data;
- the individual's right to withdraw consent; and
- the possible risks involved in making a transfer to a country which does not provide adequate protection for personal data and without any other appropriate safeguards in place. For example, you might explain that there will be no local supervisory authority, and no (or only limited) individual data protection or privacy rights.

b) **It is necessary to perform a contract**

This exception explicitly states that it can only be used for **occasional** restricted transfers. This means that the restricted transfer may happen more than once but not regularly. If you are regularly making restricted transfers, you should be putting in place an appropriate safeguard.

The transfer must also be **necessary**, which means that you cannot perform the core purpose of the contract, or the core purpose of the steps needed to enter into the contract, without making the restricted transfer. It does not cover a transfer for you to use a cloud-based IT system.

c) **It is necessary to make or defend a legal claim**

This exception explicitly states that you can only use it for **occasional** transfers. This means that the transfer may happen more than once but not regularly. If you are regularly transferring personal data, you should put in place an appropriate safeguard.

The transfer must be necessary, so there must be a close connection between the need for the transfer and the relevant legal claim.

The claim must have a basis in law, and a formal legally defined process, but it is not just judicial or administrative procedures.

5. Record keeping

It is vital in order to meet the Accountability Principle that all overseas transfers are fully documented. Such transfers must be referenced in:

- Your Privacy Notices
- Your Records of Processing Activity

- Your Risk Register
- Your Processor Evidence Files

5.1. Privacy Notices

Where you will be transferring personal data outside the UK, the law requires you to tell people this, and explain what safeguards are in place to secure the data. At the point of collection, or as soon as you receive the personal data, you must make the data subjects aware of their rights and how their data will be processed, including any overseas transfers. Privacy notices are usually held on your website, and data collection forms provide signposting to them. You must advise if personal data will be transferred or stored overseas, and which safeguard you are relying on for that processing.

Your general privacy notice must make clear how individuals can exercise their rights and how to make complaints.

5.2. Records of Processing Activity

To comply with data protection law, you must maintain records of processing activity. An element of this is the mapping of your data flows. Where data is transferred or received from overseas you must state which countries are involved. Please ensure you complete **column U (previously BF) of your RoPA** with the type of safeguard you will be using for each overseas flow.

5.3. Risk Register

Typically, the high-risk processing will involve processing of personal data that meets the requirement to undertake a Data Protection Impact Assessment (DPIA) (Document G4). The UK GDPR requires these to be undertaken by law if your proposed processing poses “a high risk to the rights and freedoms of” data subjects (Article 35).

The term “high risk” is not well defined in the law, but as a rule of thumb, wherever your proposed processing involves Special Category (sensitive personal) data, or there are other risks, e.g. overseas transfers, then undertaking the DPIA process is required. The process is a risk assessment, prompting you to consider how your new service or system is going to remain compliant with the law. It will capture the details of the safeguards you will apply to overseas transfers. Use document G5 to guide you through the risk assessment.

Before you decide on an appropriate safeguard for overseas processing, you must carry out a TRA. The TRA is an interactive assessment which helps you assess the risks to individuals rights and their access to redress should a breach occur. It is focussed on both security and human rights and requires an assessment of the domestic laws and current human rights performance of the receiving country.

It is advisable to engage with your Data Protection Officer (DPO) as early as possible in this process as the law requires the School to seek the DPO's advice. There should be evidence of the DPO's involvement, e.g. an approval 'sign-off' in order to satisfy the legal requirement.

5.4. Processor Evidence Files

Where your suppliers provide services, e.g. hosted solutions, overseas you must ensure that there is a formal contract. Where the recipient/sender country does not have an adequacy decision you will need to complete a Transfer Risk Assessment and use an appropriate safeguard, e.g. the International Data Transfer Agreement. You should keep all documentation for all Processors in an Evidence File (or collection of files) for ease of review.

6. Advice and Support

If you have any issues over the clarity of these procedures, how they should be applied in practice, require advice about exemptions from the requirements or have any suggestions for amendments, please contact the school office.

7. Breach Statement

A breach of this procedure is a breach of Information Policy. Breaches will be investigated and may result in disciplinary action. Serious breaches of Policy may be considered gross misconduct and result in dismissal without notice, or legal action being taken against you.

Annex A: Overseas Transfer Mechanisms

- [Regulatory advice](#)
- [Transfer Risk Assessment](#)
- [US Data Privacy Framework](#)
- [International data transfer agreement \(PDF\)](#)
- [International data transfer agreement \(Word document\)](#)
- [International data transfer addendum to the European Commission's standard contractual clauses for international data transfers \(PDF\)](#)
- [International data transfer addendum to the European Commission's standard contractual clauses for international data transfers \(Word document\)](#)