# Data Protection Policy

## Contents



.

# 1. Introduction

The Dragon Trip is committed to protecting the privacy and confidentiality of personal data collected and processed in the course of our business operations.

This Data Protection Policy outlines our practices and procedures for handling personal data in compliance with applicable data protection laws and regulations.

## 2. Scope of this policy

The Dragon Trip needs to comply with the Data Protection Act 2018 and EU General Data Protection Regulations. This policy applies to all employees, contractors, and third parties who handle personal data on behalf of The Dragon Trip.

It applies to all personal data collected, stored, processed, or transmitted in any format, including electronic and physical records.

This policy has been developed to ensure all staff, contractors and partners understand their obligations when processing personal and special category data. So long as the processing of the data is carried out for company purposes, it applies regardless of where the data is held.

'Processing' data is widely defined and includes obtaining, recording, keeping, or using it in any way; sharing or disclosing it; erasing and destroying it.

## 3. Data protection principles

Personal and special category data must be:

**3.1 Lawfulness, Fairness, and Transparency**

Personal data will be processed lawfully, fairly, and transparently. Data subjects will be informed of the purposes and legal basis for the processing of their personal data.

**3.2 Used for a specific purpose**

The data must be collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes.

**3.3 Be relevant to the purpose**

The data must be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed

**3.4 Be accurate**

Data should be 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

**3.5 Storage Limitation**

Personal data will be retained only for as long as necessary to fulfill the purposes for which it was collected. All staff members holding files containing personal information must permanently delete data within 3 months of their trip finishing. Unless a longer retention period is required by law.

**3.6 Kept securely**

Appropriate technical and organizational measures will be implemented to ensure the security of personal data and to protect it against unauthorized or unlawful processing, accidental loss, destruction, or damage.

Personal data should be password protected, and the documents and passwords should only be shared with staff members or suppliers who need it to perform job functions.

**3.7 Data Subject (Customers) Rights**

Data subjects will be provided with information about their rights regarding their personal data, including the right to access, rectify, erase, restrict processing, object to processing, and data portability.

**3.8. Accountability**

The Dragon Trip is responsible for ensuring compliance with this policy. Employees and contractors are required to comply with this policy and report any data protection concerns to the Central Service Department.

## 4. Data Collection and Processing

**4.1. Lawful Basis**

Personal data will be collected and processed based on a lawful basis, such as the necessity of processing for the performance of a contract, compliance with legal obligations, consent, or legitimate interests pursued by The Dragon Trip or a third party.

**4.2. Consent**

Where consent is relied upon as the lawful basis for processing personal data, it will be obtained freely, and data subjects will have the right to withdraw consent at any time.

**4.3. Data Subject Rights**

Data subjects will be provided with information on how to exercise their rights regarding their personal data, and requests to exercise these rights will be handled promptly and in accordance with applicable laws.

## 5. Data Sharing and Transfers

**Third-Party - Suppliers**

Personal data may be shared with third-party suppliers who provide services to The Dragon Trip. These suppliers will be selected carefully, and appropriate safeguards, such as data processing agreements, will be in place to ensure the protection of personal data.

## 6. Data Breach Management

**What is a data breach?**

A data breach means a breach of security leading to the accidental or unlawful destruction, loss, alteration, or unauthorized disclosure of, or access to, personal data. This includes breaches that are the result of both accidental and deliberate causes. It also means that a breach is more than just about losing personal data.

**Example**

- access by an unauthorized third party;
- deliberate or accidental action (or inaction) by a controller or processor; Eg posting a private doc to a public domain
- sending personal data to an incorrect recipient;
- computing devices containing personal data being lost or stolen;
- alteration of personal data without permission; and
- loss of availability of personal data.

In the event of a personal data breach (data is leaked, damaged or lost) The Dragon Trip will promptly assess the risk to individuals' rights and freedoms and, initiate an emergency plan and take remedial measures. If required by law, notify the relevant supervisory authority and affected data subjects.

**Training and Awareness**

Regular training and circulars will be provided to employees and contractors to ensure their understanding of this policy and their responsibilities in protecting personal data.

**Policy Review**

This Data Protection Policy will be reviewed annually and updated as necessary to ensure continued compliance with applicable data protection laws and regulations.

## 7. Personal data in the public domain

The Dragon Trip holds certain information about people in the public domain, for example the staff name will be on the website. Personal data classified as being in the ‘public domain’ refers to information which will be publicly available world-wide and may be disclosed to third parties without recourse to the data subject.

## 8. Data security

Keeping personal data properly secure is vital in complying with the Data Protection Act. All staff and contractors are responsible for ensuring that any personal data we have access to is kept securely. We are also responsible for ensuring that personal data is not disclosed inappropriately (either orally or in writing or accidentally) to any unauthorised third party.

This includes, as a minimum:

- We should always keep passwords safe and never share them. Follow the guidance on creating safe passwords
- Lock away any personal data kept in paper format in a lockable cabinet or pedestal. Do not leave documents on desks unattended at any time. All staff should maintain a clean desk policy to ensure no personal data is left unattended.
- If it is necessary to take hard copy documents out of the office make sure that those documents are looked after at all times, this includes note books and files. Consider whether it is necessary to take files out of the office at all or if so, take them on an encrypted handheld device or laptop.
- If data has to go onto a disc or memory stick make sure that the device that used is encrypted and that the data is password protected.
- If we have access to these devices make sure that they are stored securely and locked away safely when not being used.

The above steps must be explained to all suppliers we send customers personal information to and suppliers must confirm that they will also comply with the same policies. If they refuse, you may not share customers data with this supplier, and must refer the situation to Central Service Team

## 9. Sending personal data securely

We can send documents containing personal data securely using the following methods:

| Requested by: | Method: |
|---|---|
| Hard copy | Documents should be hand delivered to the data subject wherever possible. Check ID and address for sending before handing over documents. Make sure that the documents are securely contained in a sealed envelope.<br><br>If it not possible for the data subject to collect the documents themselves use the **special delivery service** and include the name of the data subject on the envelope to ensure that they sign for the documents.<br>**Note:** Check you have the correct address before posting |

| | |
|---|---|
| Encrypted device | Where the data is especially sensitive consider saving the documents on a password protected, encrypted memory device rather than posting hard copies. The password can be sent to the data subject once they have<br>Received the device by post to ensure that only they have access. |
| Email | This is the preferred method. Scan a copy of the file and move it to a secure location on the office network. Send the file by secure data transfer.<br><br>Ask the data subject to confirm receipt of the documents as soon as possible. |

## 10. Prohibited activities

The following activities are strictly prohibited when processing personal and special category data:

- Sharing personal data that are not password protected. Here are some options (Password protect a PDF online for free | Adobe Acrobat, Protect a document with a password - Microsoft Support, Protect an Excel file - Microsoft Support)
- Sending personal data to a personal email address to work on at home
- Sending data to unauthorised personal. Always check that the recipients are authorised to view the information being sent
- Sending personal data in an insecure format
- Losing or misplacing personal and sensitive data
- Leaving personal data unprotected
- Accessing information about a customer or member of staff where there is no legitimate reason for doing do
- Accessing personal data about an individual for personal use
- Disclosing personal data to a third person outside of the office without a lawful basis

**It is a condition of employment in the case of staff and contractors that they abide by the law and the policies of the company. Any breach of this policy could be considered to be a disciplinary offence and may lead to disciplinary action. A serious breach of the Data Protection Act may also result in the company and/or the individual being held liable in law.**

## 11. Emergency Plan when there is a breach

A data breach may occur by accidentally sending an email to the wrong person or leaving a file in a public place. Breaches which result in a high risk to the individual must be reported to the Central Service Department within 72 hours.

If the breach is likely to result in a high risk of adversely affecting individuals' rights and freedoms, the senior management must also inform those individuals without undue delay.

It is vital for the company to have robust breach detection, investigation and internal reporting procedures in place. This will facilitate decision-making about whether or not you need to notify the relevant supervisory authority or the affected individuals, or both.

The Central Service Department will keep a record of any personal data breaches, regardless of whether we are required to notify.

The Central Service department will follow the ICO guide on handling Personal data breaches: a guide | ICO

## 12. Conclusion

Compliance with the Data Protection Policy is the responsibility of all members of staff and contractors. Any questions about this policy or any queries concerning data protection matters should be raised with the Central Service Department

## 13. Definitions

| | |
|---|---|
| Personal Data | Personal data means data which relate to a living individual who can be identified directly or indirectly from the data, particularly be reference to an identifier.<br>Personal data can be factual (such as a name, address or date of birth) or it can be an opinion (such as a performance appraisal).<br>Examples of personal data are the name and address of an individual; email and phone number |
| Special Category | Certain personal data, special category data, is given special protections under the policy because misuse could create more significant risks to a person's fundamental rights and freedoms. For example, by putting them at risk of unlawful discrimination.<br>Information relating to criminal activities or convictions is not special category data but must be treated with similar safeguards in place.<br>Special category data includes:<br>• race or ethnic origin of the data subject<br>• their political opinions<br>• their religious beliefs or other beliefs of a similar nature<br>• whether they are a member of a trade union<br>• their physical or mental health or condition<br>• their sexual life<br>• sexual orientation<br>• Biometrics (where used for ID purposes)<br>• Genetics |
| Confidential Data | Data given in confidence or data which is confidential in nature and that is not in the public domain.<br>Some confidential data will also be personal data and/or special category data and therefore come within the terms of this policy.<br>Staff handling confidential data regularly and must be careful not to disclose this information incorrectly. |
| Data Controller | The organization that determines the purposes and the manner in which any personal data is processed is known as the data controller.<br>The Dragon Trip is the data controller of all personal data used and held by the school. |

| | |
|---|---|
| Supplier | Organisations or individuals who process personal data on behalf of the data controller (The Dragon Trip) are known as Suppliers. Employees of data controllers are excluded from this definition but it could include suppliers which handle personal data on our behalf. |
| Data Subject | A living individual who is the subject of personal data is known as the data subject. |
| Lawful Basis | The grounds specified by the Regulations which need to be satisfied for any data processing to be legal. One ground needs to exist for processing personal data. Where special category data is processed a second ground must also exist. |
| Data Breach | A data breach is a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed. |

## 14. Contact Information

For questions or concerns regarding this Data Protection Policy or the handling of personal data, please contact the Central Service Department

Tunu Evans
Tunu.evans@thelearningadventure.com

Ramsay Kerr

Ramsay.kerr@thedragontrip.com