

# Data Processing Agreement

South West Grid for Learning



# Contents

Data Processing Agreement.....	3
1. Definitions.....	3
2. Processing of Personal Data.....	5
2.1 Roles of the Parties.....	5
2.2 Customer’s Processing of Personal Data.....	5
2.3 SWGfL’s Processing of Personal Data.....	6
2.4 Details of the Processing.....	6
2.5 Data Residency.....	6
3. Rights of the Data Subject.....	6
4. SWGfL Personnel.....	7
4.1 Confidentiality.....	7
4.2 Limitation of Access.....	7
5. Sub-processors.....	7
5.1 Appointment of Sub-processors.....	7
5.2 Performance by Sub-processor.....	8
5.3 Current Sub-processors, Notification of New Sub-processors and Objection Right.....	8
6. Security.....	9
6.1 Controls for the Protection of Personal Data.....	9
6.2 Audits.....	9
6.2.1 Scope of Audits.....	9
6.2.2. Reasonable Exercise of Rights.....	9
6.2.3. Third-Party Auditor.....	10
6.2.4. Findings.....	10
6.3 Data Protection Impact Assessment and Prior Consultation.....	10
7. Security Incident Notification.....	10
8. Government Access Requests.....	11
9. Retention of data for research and reporting purposes.....	12
10. Return and Deletion of Personal Data.....	12

11. International Provisions.....	13
11.1 Conditions for International Processing .....	13
11.2 International Data Transfer Mechanisms for Data Transfers.....	13
11.3 Conflict .....	13
12. Legal Effect.....	13
Signature Block.....	14
Schedule 1 (Description of the Processing) .....	15
List of sub-processors .....	15

# Data Processing Agreement

This Data Processing Agreement and its Exhibits (“DPA”) forms part of and is subject to the terms and conditions of the Agreement (as defined below) by and between you (“Customer”) and South West Grid for Learning Trust Ltd, Belvedere House, Woodwater Park, Pynes Hill, Exeter, EX2 5WS. A charitable trust company registered in England,

Scotland and Wales. Company Number: 5589479, Charity numbers: (England and Wales – 1120354, Scotland – SC051351), (“SWGFL”).

This DPA has been pre-signed on behalf of SWGFL. To enter into this DPA, Customer must: (a) be a customer of SWGFL; (b) complete the signature block below by signing and providing all relevant information; and (c) submit the completed and signed DPA to SWGFL at [privacy@swgfl.org.uk](mailto:privacy@swgfl.org.uk).

This DPA will only be effective (as of the Effective Date) if executed and submitted to SWGFL. Any deletions or other revisions to this DPA made by the Customer will render this DPA null and void. Customer signatory represents to SWGFL that he or she has the legal authority to bind Customer and is lawfully able to enter into this DPA. This DPA will terminate automatically upon termination of the Agreement, unless earlier terminated pursuant to the terms of this DPA.

## 1. Definitions

In this DPA (including Schedules), the following terms have the meanings set out below:

“**Controller**” means the entity which alone or jointly with others determines the purposes and means of the Processing of Personal Data. “**Data Protection Laws and Regulations**” means all laws and/or regulations applicable to SWGFL’s Processing of Personal Data under the Agreement.

“**Data Subject**” means the individual to whom Personal Data relates.

“**EU Standard Contractual Clauses**” means the Standard Contractual Clauses for the transfer of Personal Data to third countries pursuant to Regulation (EU) 2016/679 of the European Parliament and the Council (Module 2 (Transfer Controller to Processor) approved by the European Commission Implementing Decision (EU) 2021/914 of 4 June 2021, as currently set out at [https://eur-lex.europa.eu/eli/dec\\_impl/2021/914/oj](https://eur-lex.europa.eu/eli/dec_impl/2021/914/oj).

**“Personal Data”** means any information that has been provided by or on behalf of Customer to the Services that relates to an identified or identifiable natural person. 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 one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

**“Processing”** (and related verb forms) means any operation or set of operations which is performed upon Personal Data, whether or not by automatic means, such as collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, erasure or destruction.

**“Processor”** means the entity that Processes Personal Data on behalf of the Controller.

**“Public Authority”** means a government agency or law enforcement authority, including judicial authority.

**“Regulator”** means any Supervisory Authority or regulatory body with responsibility for ensuring compliance with Data Protection Laws and Regulations.

**“Security Incident”** means a confirmed or reasonably suspected accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, access to Personal Data.

**“Sub-processor”** means any third-party processor engaged by SWGfL to Process Personal Data in order to provide the Services to Customer under the Agreement and/or this DPA. For the avoidance of doubt, telecommunication providers are not Sub-processors.

**“Supervisory Authority”** means an independent public authority which is established by a member state pursuant to Article 51 of the GDPR or, for the United Kingdom, the Information Commissioner’s Office (“ICO”).

**“UK International Data Transfer Agreement”** means the International Data Transfer Addendum to the EU Standard Contractual Clauses issued by the UK Information Commissioner, Version B1.0, in force 21 March 2022.

All other capitalized definitions in this DPA not explicitly defined in this DPA, shall have the same meanings as defined in the Agreement, the GDPR or other Data Protection Laws and Regulations, in that order of precedence.

## 2. Processing of Personal Data

### 2.1 Roles of the Parties.

The parties acknowledge and agree that with regard to the Processing of Personal Data, Customer is the Controller and determines the purposes for which and the manner in which the Personal Data is Processed, SWGFL is the Processor of any Personal Data, acting on behalf of the Customer. SWGFL may engage Sub-processors pursuant to the requirements set forth in Section 5 “Subprocessors” below. Each party, in respect of the Processing of the Personal Data acknowledges and agrees that each party has respective rights and obligations under applicable Data Protection Laws and Regulations.

### 2.2 Customer’s Processing of Personal Data.

Customer shall, in its use of the Services, Process Personal Data in accordance with the requirements of Data Protection Laws and Regulations, including any applicable requirement to provide notice to Data Subjects of the use of SWGFL as Processor.

For the avoidance of doubt, Customer will ensure that its instructions for the Processing of Personal Data comply with Data Protection Laws and Regulations. Customer acknowledges that SWGFL is neither responsible for determining which laws or regulations are applicable to Customer’s business nor whether SWGFL’s provision of the Services meets or will meet the requirements of such laws or regulations.

Customer will ensure that SWGFL’s Processing of Personal Data, when done in accordance with the Customer’s instructions, will not cause SWGFL to violate any applicable law or regulation, including applicable Data Protection Laws and Regulations.

Customer shall have sole responsibility for the accuracy, quality, and legality of Personal Data and the means by which Customer acquired Personal Data. Customer shall ensure that the Customer is entitled to transfer the relevant Personal Data to SWGFL so that SWGFL and its Sub-processors may lawfully use, process and transfer the Personal Data in accordance with this DPA and the Agreement on Customer’s and its Affiliates’ behalf.

SWGFL will inform Customer if it becomes aware, or reasonably believes, that Customer’s instructions violate any applicable law or regulation, including applicable Data Protection Laws and Regulations.

## **2.3 SWGFL's Processing of Personal Data**

SWGFL shall Process Personal Data on behalf of and in accordance with Customer's written instructions and shall treat Personal Data as Confidential Information. Customer instructs SWGFL to Process Personal Data for the following purposes:

- (i) Processing initiated by Customer's Subscribers or other Data Subjects authorised to use the Services;
- (ii) Processing to comply with other reasonable instructions provided by Customer (e.g, via email) where such instructions are consistent with the terms of the Agreement and Data Protection Laws and Regulations; and
- (iii) as otherwise required by applicable law.

The Agreement and this DPA, along with Customer's configuration and use of the Services, are Customer's complete and final instructions to SWGFL in relation to the Processing of Personal Data, including for purposes of the Standard Contractual Clauses, and any Processing required outside of the scope of these instructions (inclusive of the rights and obligations set forth under the Agreement) will require prior written agreement of the parties.

## **2.4 Details of the Processing**

The subject-matter of Processing Personal Data by SWGFL is the performance of the Services pursuant to the Agreement. The duration of the Processing, the nature and purpose of the Processing, the types of Personal Data and categories of Data Subject Processed under this DPA are further specified in Schedule 1 (Description of the Processing) to this DPA.

## **2.5 Data Residency**

With respect to the Services, SWGFL may store data in the UK or European Union.

# **3. Rights of the Data Subject**

SWGFL shall, to the extent legally permitted, promptly notify Customer if it receives a complaint, dispute or request from a Data Subject such as a Data Subject's right of access, correction, amendment or deletion ("right to be forgotten"), data portability, objection to the Processing or its right not to be subject to an automated individual decision making (each such complaint, dispute or request being a "Data Subject Request").

SWGFL shall not respond to any such Data Subject Request without Customer's prior written consent except that Customer authorizes SWGFL to redirect the Data Subject Request as necessary to allow Customer to respond directly.

Taking into account the nature of the Processing and the information available to SWGfL, SWGfL assists Customer by appropriate technical and organizational measures, insofar as this is possible, for the fulfilment of the Controller's obligation to respond to a Data Subject Request under Data Protection Laws and Regulations.

As part of the Services, SWGfL provides Customer with a number of self-service features, including the ability to delete Personal Data. Customer may use these self-service features to assist in complying with its obligations under Data Protection Laws and Regulations with respect to responding to Data Subject Request via the Services at no additional cost.

In addition, to the extent Customer, in its use of the Services, does not have the ability to address a Data Subject Request, SWGfL shall, upon Customer's written request, provide Customer with commercially reasonable cooperation and assistance in responding to such Data Subject Request, to the extent SWGfL is legally permitted to do so and the response to such Data Subject Request is required under Data Protection Laws and Regulations.

If legally permitted, Customer shall be responsible for any reasonable costs arising from SWGfL's provision of such assistance, requested by Customer.

## **4. SWGfL Personnel**

### **4.1 Confidentiality**

SWGfL shall ensure that its personnel and those of its Affiliates engaged in the Processing of Personal Data are informed of the confidential nature of the Personal Data, have received appropriate training on their responsibilities and have executed written confidentiality agreements.

### **4.2 Limitation of Access**

SWGfL shall ensure that SWGfL's access to Personal Data is limited to those personnel who require such access to perform the Agreement.

## **5. Sub-processors**

### **5.1 Appointment of Sub-processors**

Customer acknowledges and agrees that SWGfL's Affiliates may be retained as Sub-processors, and SWGfL and SWGfL's Affiliates respectively may engage third-party Sub-processors in connection with the provision of the Services, in each case

- (a) anywhere in the world where SWGFL, its Affiliates or its or their Sub-processors maintain data processing operations, and
- (b) subject to a written agreement requiring the Sub-processor to comply with the requirements of applicable Data Protection Laws and Regulations and to abide by terms no less protective of the Customer Personal Data than those provided in this DPA to the extent applicable to the nature of the services provided by such Sub-processor.

## **5.2 Performance by Sub-processor**

SWGFL shall be liable for any such Sub-processor's performance of any obligation under this DPA.

## **5.3 Current Sub-processors, Notification of New Sub-processors and Objection Right**

SWGFL's current list of Sub-processors engaged in Processing Personal Data for the performance of each applicable Service, is available at [\[insert link\]](#) ("Sub-processor List").

Customer hereby consents to those Sub-processors listed in the Sub-processor List, their locations and processing activities as it pertains to the Personal Data. Customer may subscribe to updates to the relevant Sub-processor List.

If Customer subscribes, SWGFL shall provide such updates at least thirty (30) days prior to authorising any new Sub-processor(s) to Process Personal Data in connection with the provision of the Services.

If Customer has a reasonable basis to object to SWGFL's use of a new Sub-processor relating to data protection, Customer shall notify SWGFL in writing within ten (10) business days after receipt of SWGFL's notice. In such event, the parties will discuss Customer's concerns in good faith with a view to achieve resolution.

If Customer can reasonably demonstrate the new Sub-processors is unable to Process Personal Data in compliance with the terms of this DPA and SWGfL cannot provide an alternative Sub-processor, or the parties are not otherwise able to achieve resolution as provided in the preceding sentence within sixty (60) days, Customer, as its sole and exclusive remedy, may provide written notice to terminate only those specific affected elements of the Services in the applicable Ordering Document(s) which cannot be provided by SWGFL and/or a mutually agreed upon Sub-Processor without the use of the objected-to new Sub-processor.

Within thirty (30) days of receipt of such notice from Customer, Customer shall receive a refund of any prepaid fees for the period following the effective date of termination in respect of such terminated Services.

## **6. Security**

### **6.1 Controls for the Protection of Personal Data**

SWGFL shall maintain appropriate administrative, physical and technical safeguards for protection of the security, confidentiality and integrity of Personal Data that are appropriate to (a) the size, scope and type of SWGFL's business; (b) the amount of resources available to SWGFL; (c) the type of information that SWGFL will store; and (d) the need for security and confidentiality of such information. SWGFL shall regularly monitor compliance with these safeguards.

### **6.2 Audits**

Customer may contact SWGFL to request an audit of SWGFL's Processing activities covered by this DPA ("Audit").

#### **6.2.1 Scope of Audits**

Audits will be limited to Personal Data Processing and storage facilities operated by SWGFL or any of SWGFL's Affiliates.

Customer acknowledges that SWGFL shall have the right to reasonably adapt the scope of any Audit to avoid or mitigate risks with respect to, and including, service levels, availability, and confidentiality of other SWGFL customers' information.

#### **6.2.2. Reasonable Exercise of Rights**

An Audit shall be conducted by Customer or its Third-Party Auditor:

- (i) acting reasonably, in good faith, and in a proportional manner, taking into account the nature and complexity of the Services used by Customer;
- (ii) up to one time per year with at least four (4) weeks' advance written notice. If an emergency justifies a shorter notice period, SWGFL will use good faith efforts to accommodate the Audit request; and
- (iii) during SWGFL's normal business hours, under reasonable duration and shall not unreasonably interfere with SWGFL's day-to-day operations.

Before any Audit commences, Customer and SWGFL shall mutually agree upon the scope, timing, and duration of the audit and the reimbursement rate for which Customer shall be

responsible. All reimbursement rates shall be reasonable, taking into account the resources expended by or on behalf of SWGfL.

### **6.2.3. Third-Party Auditor**

A Third-Party Auditor means a third-party independent contractor that is not a competitor of SWGfL. An Audit can be conducted through a Third-Party Auditor if:

- (i) prior to the Audit, the Third-Party Auditor enters into a non-disclosure agreement containing confidentiality provisions no less protective than those set forth in the Agreement to protect SWGfL's proprietary information; and
- (ii) the costs of the Third-Party Auditor are at Customer's expense.

### **6.2.4. Findings**

All information gathered during the Audit as the audit report created from the Audit is confidential and cannot be divulged to third parties (unless mandated by applicable law) without SWGfL's prior written consent. Customer must promptly provide SWGfL with information regarding any non-compliance discovered during the course of an Audit.

## **6.3 Data Protection Impact Assessment and Prior Consultation**

So long as Customer does not otherwise have access to the relevant information, and to the extent such information is available to SWGfL, SWGfL shall provide reasonable assistance to Customer needed to fulfil Customer's obligation under Data Protection Laws and Regulations to carry out a data protection impact assessment related to Customer's use of the Service (at Customer's expense only if such reasonable cooperation will require SWGfL to assign significant resources to that effort).

## **7. Security Incident Notification**

SWGfL has implemented and will maintain security incident management policies and procedures as set forth in the Agreement.

SWGfL shall, to the extent permitted by law, notify Customer's designated contact as set forth by Customer in the signature block below, without undue delay (and in any event within 72 hours of confirmation), after SWGfL's discovery of a Security Incident") impacting Personal Data of which SWGfL is a Processor.

Any such notification is not an acknowledgement of fault or responsibility. SWGfL shall make reasonable efforts to identify a Security Incident and, to the extent a Security Incident is caused by a violation of the requirements of this DPA by SWGfL, remediate the cause of such

Security Incident. SWGfL will reasonably assist the Customer to comply with its reporting obligations under applicable Data Protection Laws and Regulations in connection with the Security Incident.

In case of a Security Incident and prior to making any required public statement or required notice, Customer agrees to timely provide SWGfL with a draft for discussion on the content of its intended required public statements or required notices for the affected Data Subjects and/or required notices to the relevant Regulators regarding the Security Incident to the extent such public statements or notices identify SWGfL by name or relate to SWGfL's software and/or Services.

This draft shall be discussed in a timely fashion and in good faith between the parties. Notwithstanding the preceding sentence, Customer shall not be required to prejudice its obligations under Data Protection Laws and Regulations.

## **8. Government Access Requests**

In its role as a Processor, SWGfL shall maintain appropriate measures to protect Personal Data in accordance with the requirements of Data Protection Laws and Regulations, including by implementing appropriate technical and organizational safeguards to protect Personal Data against any interference that goes beyond what is necessary in a democratic society to safeguard national security, defence and public security.

If SWGfL receives a legally binding request to access Personal Data from a Public Authority, SWGfL shall, unless otherwise legally prohibited, promptly notify Customer including a summary of the nature of the request.

To the extent SWGfL is prohibited by law from providing such notification, SWGfL shall use commercially reasonable efforts to obtain a waiver of the prohibition to enable SWGfL to communicate as much information as possible, as soon as possible.

Further, SWGfL shall challenge the request if, after careful assessment, it concludes that there are reasonable grounds to consider that the request is unlawful. SWGfL shall pursue possibilities of appeal.

When challenging a request, SWGfL shall seek interim measures with a view to suspending the effects of the request until the competent judicial authority has decided on its merits. It shall not disclose the Personal Data requested until required to do so under the applicable procedural rules. SWGfL agrees it will provide the minimum amount of information

permissible when responding to a request for disclosure, based on a reasonable interpretation of the request.

SWGfL shall promptly notify Customer if SWGfL becomes aware of any direct access by a Public Authority to Personal Data and provide information available to SWGfL in this respect, to the extent permitted by law. For the avoidance of doubt, this DPA shall not require SWGfL to pursue action or inaction that could result in civil or criminal penalty for SWGfL such as contempt of court.

## **9. Retention of data for research and reporting purposes**

SWGfL will make use of any information provided in our tools for research purposes including, but not limited to, the reporting of national aggregated results. In order to conduct research and compile annual reports Customer data will be shared with trusted academic teams in accordance with this agreement.

Customer data will only be publicly referenced in an aggregated form and will not be attributed to a single entity. Personal data provided in our tools will not feature in public reporting or research outcomes.

## **10. Return and Deletion of Personal Data**

SWGfL shall make Personal Data available for export by Customer upon written request made within thirty (30) days of the date of termination/expiration of the Agreement. Unless prohibited by applicable law, within one hundred twenty (120) days after the termination/expiration of the Agreement, SWGfL shall securely destroy all Personal Data in its possession or control.

Notwithstanding anything to the contrary in this Section 8, SWGfL may retain Personal Data, or any portion of it, if required by applicable law or regulation or in furtherance of the Agreement, including Data Protection Laws and Regulations or for electronic backups, provided such Personal Data remains protected in accordance with the terms of the Agreement, this DPA and the Data Protection Laws and Regulations.

## 11. International Provisions

### 11.1 Conditions for International Processing

SWGFL shall be entitled to Process Personal Data, including by using Sub-processors, in accordance with this DPA outside the country in which the Customer is located as permitted under Data Protection Laws and Regulations.

### 11.2 International Data Transfer Mechanisms for Data Transfers

To the extent Customer's use of the Services requires an onward transfer mechanism to lawfully transfer Personal Data from a jurisdiction (i.e., the EEA, the United Kingdom, to SWGFL or its Sub-processor located outside of that jurisdiction ("Transfer Mechanism")), the terms set forth in Schedule 2 "International Transfer Mechanisms" will apply.

### 11.3 Conflict

In the event of any conflict or inconsistency among the following documents, the conflict or inconsistency shall be resolved by giving precedence in the following order:

- (i) the applicable Data Protection Laws and Regulations;
- (ii) the EU Standard Contractual Clauses or the UK International Data Transfer Agreement as applicable; and
- (iii) this DPA.

## 12. Legal Effect

This DPA shall only become legally binding between the eligible Customer and SWGFL when each of the steps set out in the Section "HOW TO EXECUTE THIS DPA" above have been fully completed.

The terms of this DPA will end simultaneously and automatically with the termination of the Services by the Customer or SWGFL however any obligation imposed on SWGFL under this DPA in relation to the Processing of Personal Data shall survive any termination or expiration of the Agreement for as long as SWGFL maintains such Personal Data in its possession.

This DPA is part of and subject to the terms of the Agreement. Customer's remedies (including those of its Affiliates) with respect to any breach by SWGFL of the terms of this Agreement will be subject to any aggregate limitation of liability that applies to the Customer under the Agreement.

With regard to the subject matter of this DPA, in the event of inconsistencies between the provisions of this DPA and the Agreement, the provisions of this DPA shall prevail with regard to the parties' data protection obligations.

## Signature Block

Signed by George Martin, Security and Data Protection Advisor, SWGfL

*George Martin*

Signed by Customer:

Name: .....

Role: .....

Organisation: .....

Note that the person signing this on behalf of the organisation should also be an administrator of the SWGfL tool purchased.

# Schedule 1 (Description of the Processing)

## List of sub-processors

Name of service	Personal data processed	Description of processing	Data storage location
SWGfL website	Data Subject DS category	collection, access, structuring, storage, use, erasure or destruction	IONOS - UK
360 family websites 360Groups 360Earlyyears 360safe 360safecymru 360safescotland 360digi Computing Quality Framework	Data Subject DS category	collection, access, structuring, storage, consultation, use, disclosure by transmission, erasure or destruction	IONOS - UK
Boost	Data Subject DS category	collection, access, structuring, storage, use, erasure or destruction	IONOS - UK
Whisper	Data Subject DS category Student S category Sensitive	collection, access, structuring, storage, use, disclosure by transmission, erasure or destruction	IONOS - UK
SWGfL store (Powered by Shopify)	Data Subject DS category	collection, access, structuring, storage, use, disclosure by transmission, erasure or destruction	

<b>The Revenge Porn Helpline</b>	Data Subject DS category Sensitive	collection, access, structuring, storage, consultation, use, disclosure by transmission, erasure or destruction	IONOS - UK
<b>The Report Harmful Content website</b>	Data Subject DS category Student S category Sensitive	collection, access, structuring, storage, consultation, use, disclosure by transmission, erasure or destruction	IONOS - UK
<b>The Test Filtering website</b>	Data Subject DS category	collection, access, structuring, storage, use, disclosure by transmission, erasure or destruction	IONOS - UK
<b>Project Evolve</b>	Data Subject DS category Student S anon	collection, access, structuring, storage, consultation, use, disclosure by transmission, erasure or destruction	IONOS - UK
<b>Microsoft – Azure and Office 365</b>	Data Subject DS category	We use Azure and Office365 to store files and send emails. This system may be used to analyse data from our web systems in order to undertake research or for performance assessment	United Kingdom
<b>Google Drive</b>	Data Subject DS category	We use Google Drive to host the slides and worksheets used in Project Evolve. ProjectEVOLVE does not store any personal data in Google Drive	Global

<b>Zendesk</b>	Data Subject DS category Student S category Sensitive	Zendesk is a customer relationship management tool that we use to store any incoming case information, either from your email to us, or our practitioner entering text into the system to create a case. This information will be used to anonymously analyse and report on Helpline performance and identify trends and issues.	Dublin
<b>Salesforce</b>	Data Subject DS category	We share your details with Salesforce so that we can manage your subscriptions and contact you easily.	Frankfurt, requested move to UK
<b>Google Analytics</b>	Data Subject DS category Student S category Sensitive	We use Google Analytics for performance monitoring our systems by collecting anonymous usage data. You may optout of the use of these cookies.	Global
<b>RM Education</b>	Data Subject DS category	We share customer (school/staff) information with RM to enable the resolution of outage/technical issues relating to their Schools internet service	EEA/UK/Outside EEA for order fulfillment or processing.
<b>3CX</b>	Data Subject DS category Student S category Sensitive	SWGfL uses 3cx to provide our virtual telephone services. This system allows us to remotely answer calls without having to be in a fixed location.	London

<b>CloudAlly</b>	Data Subject DS category	We use CloudAlly as an intermediary to enable us to routinely backup our Salesforce data. CloudAlly provides a cloud-to-cloud secure backup process.	EU or adequacy approved location
<b>IONOS</b>	Data Subject DS category Student S category Sensitive	Our third party datacentre is provided by IONOS and is hosted in the UK. We use IONOS servers to provide all our WebApps. Our websites store data you provide to us on a server in the IONOS datacentre.	UK
<b>TextAnywhere</b>	Data Subject DS category Students category Sensitive	SWGfL uses TextAnywhere to provide our text messaging services. Contact details you share with us may be transferred to TextAnywhere in order that we can contact you via SMS message.	UK/EEA unless Adequacy
<b>SendGrid</b>	Data Subject DS category Student S category Sensitive	We use SendGrid as an SMTP service for bulk emails and automated emails sent by SWGfL.	Located in the US, but uses a UK/EU addendum.
<b>Amazon AWS</b>	Data Subject DS category Sensitive	Hosting the UK Safer Internet Centre website	Ireland

## Definitions

**Data subject** means: potential and actual employees of the customer

**Student** means: a data subject of the customer that is under the age of 18 and in full time education.

**DS Category** means: First name, last name, email address, contact information, IP address and any notes provided by the customer or SWGfL regarding the foregoing.

**S Category** means: First name, last name, email address, contact information, and any notes provided by the customer regarding the foregoing.

**S anon** means: Anonymous attainment level data about an individual student, or group of student responses to impact questions

**Sensitive** means: Any sensitive or health data provided by a customer during, or upon initiation, of a case. This may include protected characteristic information.