



Data Protection Policy

1	Purpose	3
2	Applies To	3
3	Definitions.....	3
4	Guidelines and Background	4
5	Policy Statements	4
6	Review.....	7
7	Not Used	7
8	Policy Details – Data Processing	8
9	Policy Details - Data Subject Rights	8
10	Policy Details - Legal Basis for Processing Personal Data.....	9
11	Policy Details – Personal Data Transfer	10
12	Policy Details – Information Security	11
13	Policy Details – Breach Management	11
14	Policy Details - Legislation	12
15	Policy Details - Supervisory Authority	12

1 Purpose

- 1.1 This policy describes how data will be managed and protected within the South West Grid for Learning Trust Ltd (“SWGfL”).
- 1.2 It includes:
 - 1.2.1 SWGfL’s approach to data protection; and
 - 1.2.2 Alignment of SWGfL’s approach with relevant legislation.
- 1.3 The objectives of this policy are:
 - 1.3.1 to clarify SWGfL’s commitment to data protection for SWGfL Staff, service users, customers, suppliers and other third parties;
 - 1.3.2 to provide an overview of SWGfL’s data protection processes and practices; and
 - 1.3.3 to align SWGfL’s data protection processes and practices with relevant legislation.

2 Applies To

- 2.1 This policy applies to:
 - 2.1.1 all Personal Data processed by SWGfL in the course of its business;
 - 2.1.2 all products and services developed and provided by SWGfL, to the extent that such products and services interface with point 2.1; and
 - 2.1.3 all SWGfL Staff, to the extent that such products and services interface with point 2.1.
- 2.2 It is intended for use by SWGfL, and by service users, customers, suppliers and other third parties with an interest in SWGfL’s data protection processes.

3 Definitions

The following definitions apply within this policy:

- 3.1 “Data Breach” means the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to data;
- 3.2 “Data Controller” means the person or organisation which (alone or jointly with others) determines the purposes and means of the Processing of Personal Data;
- 3.3 “Data Processor” means the person or organisation which Processes Personal Data on behalf of the Data Controller;
- 3.4 “Data Subject” means an identified or identifiable natural person, where such identification can be established using Personal Data;
- 3.5 “Freedom of Information Act (“FOIA”) Request” means a request issued pursuant to Section 1 of the FOIA and in compliance with Section 8 of the FOIA;

- 3.6 “Personal Data” means any information relating to a Data Subject 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 to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity;
- 3.7 “Personal Data Breach” means the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to Personal Data
- 3.8 “Processing” means any operation performed on Personal Data, including but not limited to collection, storing, using and/or disclosing of Personal Data;
- 3.9 “Special Category Personal Data” means Personal Data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person’s sex life or sexual orientation;
- 3.10 “Subject Access Request (“SAR”)” means a Data Subject exercising their rights pursuant to Article 15 of the GDPR; and
- 3.11 “SWGfL Staff” means all employees of SWGfL, including but not limited to employees, contractors, volunteers and Trustees).

4 Guidelines and Background

- 4.1 SWGfL needs to Process certain data in order to function, including the data needed to operate its products and services; to employ SWGfL Staff; and to comply with relevant organisational requirements.
- 4.2 SWGfL shall seek to maintain a high standard of data protection and information security.
- 4.3 SWGfL shall recognise, observe and protect the rights of Data Subjects in regard to any of their Personal Data that SWGfL Processes, in accordance with all applicable legal, regulatory and contractual obligations.
- 4.4 SWGfL shall support its data protection policies, processes and practices with relevant review and assurance processes (e.g. [Cyber Essentials](#)).

5 Policy Statements

- 5.1 SWGfL Products and Services
 - 5.1.1 SWGfL shall seek to ensure that its products and services maintain a high standard of data protection.
 - 5.1.2 SWGfL shall develop products and services using principles of data protection by design and data protection by default.
 - 5.1.3 Certain SWGfL products and services may undertake Processing of Special Category Personal Data. Such Processing shall be subject to additional processes and safeguards.

5.2 Data Controller

5.2.1 SWGfL shall act as the Data Controller where:

5.2.1.1 the Data Subject is (or has been) SWGfL Staff, and prospective SWGfL Staff;

5.2.1.2 the Data Subject is using (or is intending to use) a SWGfL product or service as a private individual (and not as described in point 5.3); and

5.2.1.3 the Data Subject is receiving (or is intending to receive) information from SWGfL through one or more of the following channels:

- a) SWGfL website(s), as defined in the SWGfL Privacy Notice (at www.swgfl.org.uk/terms);
- b) SWGfL email marketing and communications, including but not limited to newsletters sent by SWGfL; and
- c) SWGfL events, which may be run by SWGfL or on SWGfL's behalf.

5.3 Data Processor

5.3.1 SWGfL shall act as the Data Processor where:

5.3.1.1 the Data Subject is employed by (including but not limited to employees, contractors, volunteers and directors) an organisation that is using (or is intending to use) a SWGfL product or service;

5.3.1.2 the Data Subject attends an organisation as part of their education that is using (or is intending to use) a SWGfL product or service;

5.3.1.3 the Data Subject is employed by (including but not limited to employees, contractors, volunteers and directors) an organisation that is supplying (or is intending to supply) SWGfL with a product or service or working (or intending to work) with SWGfL in the course of their business; and

5.3.1.4 the Data Subject is a third party.

5.4 Data Processing

5.4.1 SWGfL shall Process Personal Data only where there is a legitimate requirement to do so.

5.4.2 SWGfL shall undertake Data Processing in accordance with section 8.

5.5 Data Subject Rights

5.5.1 SWGfL shall recognise, observe and protect the rights of Data Subjects in Processing Personal Data.

5.5.2 SWGfL shall interface the rights of Data Subjects with its data protection policies, processes and practices in accordance with section 9.

5.6 Freedom of Information Act (FOIA) Requests

5.6.1 FOIA requests shall be managed in accordance with the SWGfL SAR and FOIA Policy.

5.6.2 The SWGfL SAR and FOIA Policy shall observe any relevant guidance from the ICO.

5.7 Subject Access Requests

5.7.1 SARs shall be managed in accordance with the SWGfL SAR and FOIA Policy.

5.7.2 The SWGfL SAR and FOIA Policy shall observe any relevant guidance from the ICO.

5.8 Data Retention

5.8.1 SWGfL shall retain Personal Data only for as long as it is required for legitimate purposes and in accordance with section 10.

5.8.2 The retention periods for Personal Data shall take in to account any contractual requirements, relevant available guidance (statutory and non-statutory), and the nature of the product and/or service to which the Personal Data is related.

5.8.3 The retention periods for Personal Data and other data shall be set out in the SWGfL Data Retention Policy.

5.8.4 SWGfL shall retain other data which is not Personal Data in accordance with the SWGfL Data Retention Policy.

5.9 Personal Data Transfers

5.9.1 SWGfL shall not transfer Personal Data without appropriate assurances from the party to which the Personal Data shall be transferred.

5.9.2 SWGfL shall undertake any transfers of Personal Data in accordance with the provisions of section 11.

5.10 Information Security

5.10.1 SWGfL shall employ suitable measures and controls to ensure an appropriate standard of information security.

5.10.2 SWGfL's information security processes shall operate in accordance with section 12.

5.11 Breach Management

5.11.1 SWGfL shall maintain suitable Data Breach management processes to ensure any suspected Data Breaches are managed effectively.

5.11.2 SWGfL's breach management processes shall operate in accordance with section 13.

5.12 SWGfL Staff and Training

5.12.1 SWGfL Staff shall observe and comply with this policy.

5.12.2 SWGfL shall conduct initial training with new SWGfL Staff.

5.12.3 SWGfL shall conduct regular training and/or awareness sessions with SWGfL Staff.

5.13 Supervisory Authority (the ICO)

5.13.1 SWGfL shall fully co-operate with the ICO.

5.13.2 SWGfL shall observe guidance issued by the ICO and, where required, integrate such guidance into its policies and processes.

5.14 Risk Management and Governance

5.14.1 SWGfL shall observe data protection as a risk (on the basis that, in the absence of other factors influencing it, the process of data protection requires ongoing review), and shall maintain it within the internal risk management systems.

5.14.2 The SWGfL Trustee Board shall review risks regularly.

6 Review

6.1 This policy is subject to annual review.

6.2 SWGfL shall publish updated versions of this policy pursuant to review or other changes made to the data protection policies, processes and practices that need to be reflected in this policy.

6.3 This version of the policy was last updated on 21 May 2018.

7 Not Used

8 Policy Details – Data Processing

- 8.1 SWGfL shall Process Personal Data only where:
- 8.1.1 the Processing is lawful, fair and transparent to the Data Subject;
 - 8.1.2 the Processing is for specified, explicit and legitimate purposes;
 - 8.1.3 the Processing is limited to adequate and relevant Personal Data;
 - 8.1.4 the Processing includes steps to ensure that Personal Data is accurate and up to date;
 - 8.1.5 the Processing is undertaken for no longer than is necessary for the purpose; and
 - 8.1.6 the Processing is undertaken with appropriate security.
- 8.2 SWGfL shall seek to demonstrate compliance with these Processing requirements.
- 8.3 SWGfL shall set out its Processing obligations in:
- 8.3.1 Contractual documentation, both for users of a SWGfL product or service and for suppliers of a product or service to SWGfL; and
 - 8.3.2 Notices, including the SWGfL Privacy Notice and SWGfL Cookie Notice.

9 Policy Details - Data Subject Rights

- 9.1 SWGfL shall recognise, observe and protect the rights of Data Subjects in accordance with guidance from the ICO (which can be found [here](#)).
- 9.2 SWGfL shall recognise, observe and protect the following rights of Data Subjects:
- 9.2.1 The right to be informed:

SWGfL observes the right of a Data Subject to be informed about how Personal Data is collected, Processed and managed. Where this right is permitted and supported by relevant Legislation, SWGfL shall seek to provide this information in a clear and transparent manner.
 - 9.2.2 The right to access:

SWGfL observes the right of a Data Subject to access Personal Data held by a Data Controller. Where this right is permitted and supported by relevant Legislation, and where SWGfL is the Data Controller, SWGfL shall provide access to the Personal Data. Where SWGfL is not the Data Controller, pursuant to a request from the relevant Data Controller SWGfL shall seek to provide the Personal Data requested in a clear and transparent manner.
 - 9.2.3 The right to object to direct marketing:

SWGfL observes the right of a Data Subject to object, particularly to automated profiling and to direct marketing. To the extent SWGfL undertakes Processing of this

nature, and where this right is permitted and supported by relevant Legislation, SWGfL shall cease to undertake the Processing.

Where SWGfL undertakes direct marketing, Data Subjects shall be provided with the ability to stop such direct marketing by unsubscribing from it.

9.2.4 the right to object to Processing:

SWGfL observes the right of a Data Subject to object to Processing undertaken on the basis of legitimate interests. To the extent SWGfL undertakes Processing on this basis, and where this right is permitted and supported by relevant Legislation, SWGfL shall cease to undertake the Processing unless compelling legitimate grounds for the Processing are established.

9.2.5 The right to erasure:

SWGfL observes the right of a Data Subject to have Personal Data provided in a structured, commonly used and machine readable form. Where this right is permitted and supported by relevant Legislation, SWGfL shall provide Personal Data in a compliant manner.

9.2.6 The right to data portability:

SWGfL observes the right of a Data Subject to have Personal Data provided in a structured, commonly used and machine readable form. Where this right is permitted and supported by relevant Legislation, SWGfL shall provide Personal Data in a compliant manner.

9.2.7 The right to object to decisions being taken by automated means:

SWGfL shall not use automated decision making where the outcomes of such decisions could have a material effect on Data Subjects.

9.2.8 The right to rectification:

SWGfL observes the right of a Data Subject to have Personal Data rectified if it is inaccurate or incomplete. Where this right is permitted and supported by relevant Legislation, SWGfL shall rectify Personal Data accordingly.

9.2.9 The right to restrict Processing:

SWGfL observes the right of a Data Subject to have Personal Data restricted or blocked from further SWGfL Processing. Where this right is permitted and supported by relevant Legislation, SWGfL shall restrict Processing accordingly.

10 Policy Details - Legal Basis for Processing Personal Data

10.1 SWGfL shall only Process Personal Data where such Processing:

- 10.1.1 has the consent of the Data Subject: in certain cases (e.g. marketing and communications), SWGfL may use this as the lawful basis for Processing; and/or

- 10.1.2 is necessary for the performance of a contract: in certain cases (e.g. where a service is provided (or intended to be provided) to an individual), SWGfL may use this as the lawful basis for Processing; and/or
- 10.1.3 is necessary for compliance with a legal obligation: in certain cases (e.g. where there is a requirement to provide certain information to a public authority), SWGfL may use this as the lawful basis for Processing; and/or
- 10.1.4 is necessary to protect vital interests of a Data Subject or another person: in certain specific cases (e.g. where a risk to the life or health of a person is identified), SWGfL may use this as the lawful basis for Processing; and/or
- 10.1.5 is necessary in the public interest: in certain specific cases (e.g. where criminal activity is suspected), SWGfL may use this as the lawful basis for Processing; and/or
- 10.1.6 is necessary for the purposes of the legitimate interests of SWGfL or a third party: (e.g. where a service is provided (or intended to be provided) to an organisation and Personal Data is required to enable that service to be provided), SWGfL may use this as the lawful basis for Processing.

11 Policy Details – Personal Data Transfer

- 11.1 SWGfL shall not provide Personal Data to third parties for commercial purposes.
- 11.2 SWGfL shall only disclose Personal Data obtained if:
 - 11.2.1 required or authorised to do so by law;
 - 11.2.2 it is necessary to enforce or apply SWGfL's terms and conditions and/or other agreements; or to protect the rights, property, or safety of SWGfL, its customers, or others;
 - 11.2.3 SWGfL sells or buys any business or assets, in which case Personal Data may be disclosed to the prospective seller or buyer of such business or assets; or if SWGfL or substantially all of its assets are acquired by a third party, in which case Personal Data held may be one of the transferred assets;
 - 11.2.4 it is required to provide a product or service; and/or
 - 11.2.5 SWGfL has the Data Subject's consent to do so.
- 11.3 SWGfL may employ third party companies and/or individuals to perform certain functions (including delivering events, sending postal mail or email, academic/research projects related to SWGfL's work, delivering certain aspects of SWGfL service(s), and processing card payments). To the extent that they require access to Personal Data (and where it is not possible to achieve the desired outcome by providing this data in an anonymised manner), SWGfL will disclose Personal Data only where:
 - 11.3.1 the third party agrees to use it only for the agreed function(s) and not for any other purposes; and
 - 11.3.2 the third party agrees to process the Personal Data in accordance with the SWGfL Privacy Notice and as permitted by the UK's data protection legislation.

- 11.4 SWGfL may use external platforms to operate certain functions. Such platforms may be located outside the [EEA](#), however any such platforms shall be compliant with the EU-U.S. Privacy Shield Framework or have equivalent levels of protection for Personal Data.

12 Policy Details – Information Security

- 12.1 SWGfL shall employ suitable measures and controls to ensure an appropriate standard of information security.
- 12.2 Where available and appropriate, services shall be used (both for purchase and for supply) that are suitably assured (e.g. certified to [ISO 27001](#)).
- 12.3 SWGfL shall employ a range of technical measures, including but not limited to:
- 12.3.1 Data encryption;
 - 12.3.2 Anti-virus and anti-malware software;
 - 12.3.3 Network security and monitoring;
 - 12.3.4 Access management; and
 - 12.3.5 Independent security review.
- 12.4 SWGfL shall employ a range of non-technical measures, including but not limited to:
- 12.4.1 Physical security controls at premises;
 - 12.4.2 IT procurement and configuration processes;
 - 12.4.3 Appropriate IT and security policies; and
 - 12.4.4 Data protection training for SWGfL Staff.

13 Policy Details – Breach Management

- 13.1 SWGfL shall maintain effective Data Breach management processes.
- 13.2 Where a Data Breach is suspected, it shall be reported to the Head of Privacy and the SWGfL IT Team immediately. Three activity streams shall commence:
- 13.2.1 Suspension: affected systems shall be isolated; auditing and logging shall be sustained; and affected accounts shall be disabled or changed;
 - 13.2.2 Analysis: should the suspected Data Breach be confirmed, the impact of the Data Breach shall be assessed (including the impact to the affected Data Subjects); the cause of the Data Breach shall be identified; and the resolution plan shall be created;
 - 13.2.3 Communication: internal and external communications shall be issued.
- 13.3 Where a Data Breach is a Personal Data Breach, and SWGfL is the Data Controller:
- 13.3.1 SWGfL shall notify the ICO within 72 hours of becoming aware of the Personal Data Breach; and

13.3.2 Where the impact assessment suggests a high risk to Data Subjects, SWGfL shall notify the affected Data Subjects without undue delay.

13.4 Where a Data Breach is a Personal Data Breach, and SWGfL is the Data Processor, SWGfL shall notify the relevant Data Controller(s) without undue delay.

14 Policy Details - Legislation

14.1 The legislation below is applicable to data protection:

14.1.1 Data Protection Act 1998;

14.1.2 Freedom of Information Act ("FOIA") 2000;

14.1.3 General Data Protection Regulation ("GDPR"), becoming part of UK law in May 2018;

14.1.4 Investigatory Powers Act 2016;

14.1.5 Privacy and Electronic Communications Regulations ("PECR") 2003;

14.1.6 Protection of Freedoms Act 2012; and

14.1.7 The Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000.

15 Policy Details - Supervisory Authority

15.1 The Supervisory Authority in respect of SWGfL is the Information Commissioner's Office ("ICO"): <https://ico.org.uk/>