

EDUCATION DEVELOPMENT TRUST

DATA PROTECTION SCHEDULES AND PROCEDURES

Maintenance

Policy owner	Data Protection Office/In House Counsel
Review	Annual
Next review	June 2022

Version Control

Version Number	Date
Version 4	June 2021

If you have questions about how to interpret this policy, please ask the Data Protection Office/In House Counsel



Contents

Schedule 1: Standard Data Protection Clause for contracts	2
Schedule 2: Standard Data Collection Form.....	3
Schedule 3: Standard Data Processing Contract	7
Schedule 4: Contract for Overseas Transfers.....	19
Schedule 5: Data Protection Impact Assessment.....	30
Schedule 6: Record of Processing Activities: Education Development Trust.....	32
Schedule 7: Website Privacy Notice.....	36
Schedule 8: Data Subject Access Request Definition and Procedure	40
Schedule 9: Data Retention	45
Schedule 10: Data Security Breach Procedures.....	48
Schedule 11: Archive Policy Statement and Procedure.....	54
Schedule 12: Marketing and Electronic Communications.....	56
Schedule 13: Annual Review Procedure	58
Schedule 14: Security	59
Schedule 15: ICO Registration.....	60
Schedule 16: Data Privacy Frequently Asked Questions (FAQs)	61

Schedule 1: Standard Data Protection Clause for contracts

All contracts entered into by Education Development Trust will contain the standard clause at Schedule 1 regarding data protection.

(subject to amendment for the appropriate wording and definitions etc)

“The Supplier shall:

- (a) Process the Personal Data only in accordance with instructions from Education Development Trust to perform its obligations under this Agreement;
- (b) ensure that at all times it has in place appropriate technical and organisational measures to guard against unauthorised or unlawful Processing of the Personal Data and/or accidental loss, destruction, or damage to the Personal Data;
- (c) not disclose or transfer the Personal Data to any third party or Supplier Personnel unless necessary for the provision of the Services and, for any disclosure or transfer of Personal Data to any third party, obtain the prior written consent of Education Development Trust (save where such disclosure or transfer is specifically authorised under this Agreement);
- (d) take reasonable steps to ensure the reliability and integrity of any Supplier Personnel who have access to the Personal Data and ensure that the Supplier Personnel are aware of and comply with the Suppliers duties under this clause.”

Schedule 2: Standard Data Collection Form

Introduction

Unless it is not possible, not practicable, not reasonable or appropriate, or not within Education Development Trust's responsibility to ensure that it is done, the Standard Data Collection Form at Schedule 2 will be provided to each individual from whom personal data is collected. The signed Form will be stored by the business unit's Data Protection Lead and kept for as long as the personal data collected is held or processed by Education Development Trust. After that time, it will be destroyed.

If a person does not sign the Form or does not consent to the processing as detailed within it, their personal data will not be processed unless the Data Protection Lead, in consultation where necessary with the Data Protection Officer, is satisfied that an exemption exists that would allow Education Development Trust to do so without consent.

Children's Data

It is Education Development Trust's procedure that we will require parental consent, using the Standard Data Collection Form, for any processing of children's data if they are under 16.

If it is not possible, appropriate or practicable to obtain that consent, the Data Protection Lead for the unit or group must be consulted. It may be that compliance with a legal obligation, vital interests, or possibly even legitimate interests will mean that parental consent is not required in the particular circumstances, but this is to be decided on a case by case basis by the Data Protection Lead who may seek the guidance of the Data Protection Officer.

Standard Data Collection Form

The General Data Protection Regulation 2017 requires Education Development Trust to provide you with certain information when you have provided it with personal data.

'Personal data' means information relating to an identified or identifiable living person.

Please read the following information carefully and, if you agree to the use of your personal data in the manner this form describes, please sign the statement below and return it to Education Development Trust at the address shown.

Confirmation

I agree to the use of my personal data as described in this Standard Data Collection Form.

Signed: _____

Name: _____

Please return this completed form to Education Development Trust at:

Name: _____

Email: _____

Address: _____

Who are we?

Education Development Trust is a registered charity and company limited by guarantee, incorporated in England and Wales. It is a 'controller' under the General Data Protection Regulation. Occasionally it will also act as a 'processor' and if we are acting as a processor then the controller will be listed below or provided to you orally or through email at the time of collection of the data:

Controller: _____

What information will we collect from you?

We will only collect information from you that is relevant to the circumstances in which we are working with you. In particular, we may collect the following information from you which is defined as 'personal data':

Personal details – name, address, contact details; Family, lifestyle and social circumstances; Financial details; Business activities; Training needs and details of past training; Education and employment details; Goods or services provided; lifestyle and social circumstances; visual images, personal appearance and behaviour; behaviour and standards of work or performance; time logs

You will be informed of any other data we collect orally or through email at the time of collection of the data.

We may also need to collect information that is referred to as being in a 'special category'. This could include:

Racial or ethnic origin, disability information, marriage status, sexual orientation, mental or physical health, religious beliefs, trade union memberships, criminal convictions, political opinions

How will we use your information?

We may use your information to enable us, through our arrangements with you, to meet our charitable objectives through our various legitimate business concerns and commercial activities. In particular your data may be used to help us to provide education or services in the field of education or a similar field; training to our customers and clients; to promote and provide our services; to maintain our own accounts and records and to support and manage our employees, any of which may be necessary for the performance of any contract or arrangement between us. We may also use it for:

Administering any accounts; processing bank details for payment purposes; the prevention or detection of fraud; market research; marketing; Disclosure and Barring Service checks; credit reference checks

You will be informed of any other use of the data we collect orally or through email at the time of collection of the data.

Who will we share your information with?

We sometimes need to share the personal information we process with other organisations with whom we work to deliver the activities described under the paragraph "*How will we use your information?*" What follows is a description of the types of organisations we may need to share some of the personal information we process with for one or more reasons.

Business associates, clients, local authorities, charities; professional advisers; educators and examining bodies; current, past or prospective employers; family, associates and representatives of the person whose personal data we are processing; employment and recruitment agencies; financial organisations; credit reference agencies; debt collection and tracing agencies; suppliers and service providers; persons making an enquiry or complaint; other companies in the same group; central government; police forces, courts

You will be informed of any other data we collect orally or through email at the time of collection of the data.

For how long will we keep your information?

We will keep your information throughout the period of time that we work with you and for the duration of any project or association with us as part of which you provided the personal data, and for a period of six years from that point or until it is no longer necessary for us to hold the data.

Will my data be transferred outside the European Economic Area?

Our data servers or those which host our software are or may be located in the United States and so your data is likely to be transferred outside the EEA under contractual arrangements with the relevant companies providing those servers or hosting services. If you have provided data to us as part of a project that is being delivered by or with or that is linked to any of our overseas offices, then we may also need to transfer your data outside the EEA.

What rights do you have?

You have a series of rights under the General Data Protection Regulation including the right to access a copy of the information we hold about you, to have data we hold erased, to restrict the use of your data, to object to marketing use of your data, the right to withdraw consent to our processing of your data, rights concerning the portability of your data. Further information on this

issue can be obtained from our Data Protection Officer at sclifton@educationdevelopmenttrust.com

Who can you complain to if you are unhappy about what we have done with your information?

If you are unhappy about how we are using your information then initially you should contact the Data Protection Officer and if your complaint remains unresolved then you can contact the Information Commissioner's Office, details available at www.ico.org.uk.

Schedule 3: Standard Data Processing Contract

Introduction

It is a requirement of Education Development Trust that when a contract involving or requiring processing of personal data on behalf of Education Development Trust is created, anyone carrying out data processing under that subcontract on Education Development Trust's behalf will:

1. Be bound to contractual clauses requiring them to perform their roles in accordance with our policies and ensuring that they provide sufficient guarantees to implement appropriate technical and organisational measures to meet the requirements of the Data Protection Act 2018 / GDPR.
2. Process data only on the instructions of Education Development Trust.
3. Commit any subcontractors to the same levels of security and confidentiality as are required of them.

To achieve this, we will always send the Standard Data Processing Contract at Schedule 3 alongside any service contract requiring the processing of personal data on behalf of Education Development Trust to the service provider to sign. If a company/person does not sign the Contract or does not commit to the processing requirements it, personal data will not be sent to them for processing unless the Data Protection Officer is satisfied that an exemption exists that would permit Education Development Trust to do so.

Example letter enclosed with the Standard Data Processing Contract

Dear Sirs,

As you will be aware, under the Data Protection Act 2018 / GDPR a data controller is only permitted to use data processors that provide sufficient guarantees to implement appropriate technical and organisational measures in order to meet the requirements of the law, and protect the rights of the data subject.

As you carry out processing activities on our behalf, we would like to put in place an additional set of clauses in order to ensure compliance with the law. We are sending this to all data processors who process data on our behalf, regardless of the existing contractual arrangements or commitments to data security, and so we would be grateful if you could return this to us as soon as possible so that we may comply with our obligations.

Where there is an existing contract in place, this agreement will refer to that contract for the details of the personal data to be processed. Where there is not, this contract will refer to the particulars of the data for processing in the Schedule.

Please return the completed contract to: by:

We look forward to hearing from you.

Yours faithfully,

THIS AGREEMENT is dated

PARTIES

- (1) Education Development Trust, of Highbridge House, 16-18 Duke Street, Reading RG1 4RU ("Education Development Trust").

- (2) [FULL COMPANY NAME] incorporated and registered in England and Wales with company number [NUMBER] whose registered office is at [REGISTERED OFFICE ADDRESS] (“Data Recipient”).

BACKGROUND

- (A) Education Development Trust is the holder of Personal Data (as defined below).
- (B) Data Recipient is
- (C) Education Development Trust wishes to share the Personal Data with Data Recipient and Data Recipient has agreed to receive the Personal Data for the Purpose (as defined below) on the terms set out in this agreement and as described in the Schedule.

AGREED TERMS

1. INTERPRETATION

- 1.1 The definitions and rules of interpretation in this clause apply in this agreement and in any other agreement between the parties.

Business Day: a day other than a Saturday, Sunday or public holiday in England when banks in London are open for business.

Certificate of Destruction: a certificate in the form as set out in Schedule 4 which certifies that all copies of the Personal Data have been destroyed by the Data Recipient.

Commencement Date: [DATE]

Data: Personal Data and the Processed Data.

Data Controller: has the meaning set out in section 1(1) of the Data Protection Act.

Data Recipient System: any information technology system or systems owned or operated by the Data Recipient to which Data is delivered or which is used in the performance of its obligations under this agreement.

Data Protection Act: Data Protection Act 1998 as amended or replaced by the Data Protection Act 2018 and the General Data Protection Regulation and any implementing or amending legislation

Education Development Trust System: any information technology system or systems owned or operated by Education Development Trust from which Data is received in accordance with this agreement.

Existing Contract: means any contract or agreement currently in place between the Data Recipient and Education Development Trust under which the Data Recipient provides services to Education Development Trust and under which personal data may be or may already have been provided to the Data Recipient.

Instruction: means the written instruction, issued by Education Development Trust to **Data Recipient**, and directing the same to perform a specific action with regard to Personal Data (including, but not limited to, depersonalising, blocking, deletion, making available).

Intellectual Property Rights: patents, utility models, rights to inventions, copyright and neighbouring and related rights, trade marks and service marks, business names and domain names, rights in get-up and trade dress, goodwill and the right to sue for passing off or unfair competition, rights in designs, database rights, rights to use, and protect the confidentiality of, confidential information (including know-how and trade secrets), and all other intellectual property rights, in each case whether registered or unregistered and including all applications and rights to apply for and be granted, renewals or extensions of, and rights to claim priority from, such rights and all similar or equivalent rights or forms of protection which subsist or will subsist now or in the future in any part of the world.

Normal Business Hours: 8.30 am to 6.00 pm GMT on a Business Day.

Personal Data: the data relating to any individual held by Education Development Trust by which a living individual may be identified and as transferred to the Data Recipient in accordance with this agreement or the Existing Contract, as more fully described in the Schedule.

Privacy and Data Protection Requirements: the DPA, the Data Protection Directive (95/46/EC), the Regulation of Investigatory Powers Act 2000, the Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000 (SI 2000/2699), the Electronic Communications Data Protection Directive (2002/58/EC), the Privacy and Electronic Communications (EC Directive) Regulations 2003 (SI 2426/2003) and all applicable laws and regulations relating to the processing of personal data and privacy, including where applicable the guidance and codes of practice issued by the Information Commissioner or any other supervisory authority, and the equivalent of any of the foregoing in any relevant jurisdiction.

Processing, Process and Processed: have the meaning set out in section 1(1) of the DPA

Processed Data: any Personal Data that has been Processed by the Data Recipient in accordance with this agreement.

Purpose: processing of Personal Data in England and Wales for the sole purpose of performing any Existing Contract with Education Development Trust or as specified in the Schedule.

Security Breach: any security breach relating to:

- (a) the Data reasonably determined by the Data Recipient to be sufficiently serious or substantial to justify notification to the Information Commissioner or other relevant supervisory authority in accordance with the Privacy and Data Protection Requirements; or

- (b) the Data reasonably determined by the Data Recipient to be sufficiently serious or substantial to give rise to a material risk of litigation by third parties affected by the breach.

Special Conditions: the special conditions for processing the Personal Data as set out in Schedule 3.

Term: a period of [] months commencing on the Commencement Date.

- 1.2 Clause, Schedule and paragraph headings shall not affect the interpretation of this agreement.
- 1.3 A **person** includes a natural person, corporate or unincorporated body (whether or not having separate legal personality).
- 1.4 The Schedules form part of this agreement and shall have effect as if set out in full in the body of this agreement. Any reference to this agreement includes the Schedules.
- 1.5 A reference to a **company** shall include any company, corporation or other body corporate, wherever and however incorporated or established.
- 1.6 Unless the context otherwise requires, words in the singular shall include the plural and in the plural shall include the singular.
- 1.7 Unless the context otherwise requires, a reference to one gender shall include a reference to the other genders.
- 1.8 A reference to a statute or statutory provision is a reference to it as amended, extended or re-enacted from time to time.
- 1.9 A reference to a statute or statutory provision shall include all subordinate legislation made from time to time under that statute or statutory provision.
- 1.10 A reference to **writing** or **written** includes e-mail.
- 1.11 References to clauses and Schedules are to the clauses and Schedules of this agreement and references to paragraphs are to paragraphs of the relevant Schedule.
- 1.12 Any words following the terms **including**, **include**, **in particular** or **for example** or any similar phrase shall be construed as illustrative and shall not limit the generality of the related general words.
- 1.13 In the case of conflict or ambiguity between any provision contained in the body of this agreement and any provision contained in the Schedules or appendices, the provision in the body of this agreement shall take precedence.

2. EXISTING CONTRACT

- 2.1 This Data Processing Agreement (“DPA”) reflects the parties’ agreement with respect to the terms governing the processing of Personal Data. This DPA is an amendment to any Existing Contract and is incorporated into any Existing Contract.

- 2.2 The term of this DPA shall follow the term of the Existing Contract. Terms not otherwise defined herein shall have the meaning as set forth in the Existing Contract.

3. SCOPE AND RESPONSIBILITY

- 3.1 **Data Recipient** shall process Personal Data on behalf of Education Development Trust. Processing shall include such actions as may be specified in the Existing Contract and any Instructions. Within the scope of the Existing Contract, Education Development Trust shall be solely responsible for complying with the statutory requirements relating to Data Controllers under the DPA, in particular regarding the transfer of Personal Data to the Processor.
- 3.2 **Data Recipient shall be responsible for complying with the statutory requirements relating to Data Processors under the DPA** and the Processing of Personal Data (acting as “responsible body” as defined in the DPA).
- 3.3 Based on this responsibility, Education Development Trust shall be entitled to demand the rectification, deletion, blocking and making available of Personal Data during and after the term of the Existing Contract.
- 3.4 The regulations of this DPA shall equally apply if testing or maintenance of automatic processes or of Processing equipment is performed on behalf of Education Development Trust, and access to Personal Data in such context cannot be excluded.
- 3.5 The Data Recipient shall Process the Personal Data for the Purpose only and in compliance with the instructions.
- 3.6 Education Development Trust acknowledges that the Data Recipient is under no duty to investigate the completeness, accuracy or sufficiency of the Personal Data.

4. OBLIGATIONS OF DATA RECIPIENT

- 4.1 **Data Recipient** shall collect, process and use Personal Data only within the scope of Education Development Trust’s Instructions. If the **Data Recipient** thinks that an instruction of Education Development Trust infringes the DPA or other data protection provisions, it shall point this out to Education Development Trust without delay.
- 4.2 Within **Data Recipient’s** area of responsibility, **Data Recipient** shall structure its internal corporate organisation to ensure compliance with the specific requirements of the protection of Personal Data under the DPA. Processor shall take the appropriate technical and organisational measures to adequately protect Education Development Trust’s Personal Data against misuse and loss in accordance with the requirements of the DPA. Such measures hereunder shall include, but not be limited to:
- a) the prevention of unauthorised persons from gaining access to Personal Data Processing systems (physical access control),

- b) the prevention of Personal Data Processing systems from being used without authorisation (logical access control),
- c) ensuring that persons entitled to use a Personal Data Processing system gain access only to such Personal Data as they are entitled to accessing in accordance with their access rights, and that, in the course of processing or use and after storage, Personal Data cannot be read, copied, modified or deleted without authorisation (data access control),
- d) ensuring that Personal Data cannot be read, copied, modified or deleted without authorisation during electronic transmission, transport or storage on storage media, and that the target entities for any transfer of Personal Data by means of data transmission facilities can be established and verified (data transfer control),
- e) ensuring the establishment of an audit trail to document whether and by whom Personal Data have been entered into, modified in, or removed from Personal Data Processing systems (entry control),
- f) ensuring that Personal Data Processed are Processed solely in accordance with the Instructions (control of instructions),
- g) ensuring that Personal Data are protected against accidental destruction or loss (availability control),
- h) ensuring that Personal Data collected for different purposes can be processed separately (separation control).

4.3 The Data Recipient shall:

- a) treat any and all Data as confidential.
- b) ensure that the Data is kept secure and in an encrypted form, and shall use all reasonable security practices and systems applicable to the use of the Data to prevent, and take prompt and proper remedial action against, unauthorised access, copying, modification, storage, reproduction, display or distribution of the Data.
- c) only Process the Personal Data for the Purpose;
- d) be solely responsible for ensuring the security of the Data at all times throughout the Term of this agreement;
- e) comply with all applicable laws, including the Data Protection Act 2018, and all applicable industry guidelines and standards;
- f) not disclose the Personal Data to any person other than its employees who need to access to the Data to meet the Data Recipient's obligations under this agreement and the Data Recipient shall ensure that such employees are informed of the confidential nature of the Data, have undertaken training in the laws relating to handling of Data and are aware both of the Data Recipient's duties and their personal duties and obligations under such laws and this agreement;
- g) take reasonable steps to ensure the reliability of all its employees who have access to the Data.

- h) not retain the Data for any longer than is necessary for the Purpose;
 - i) only make copies of the Data to the extent reasonably necessary for the Purpose (which, for clarity, includes back-up, mirroring (and similar availability enhancement techniques), security, disaster recovery and testing of the Data);
 - j) not extract, re-utilise, use, exploit, redistribute, re-disseminate, copy or store the Data other than for the Purpose;
 - k) not do anything that may materially damage the reputation of Education Development Trust;
 - l) implement appropriate technical and organisational measures to protect the Data against unauthorised or unlawful Processing and against accidental loss, destruction, damage, alteration or disclosure;
 - m) not do, or cause or permit to be done, anything that may result in the Data Recipient and/or Education Development Trust being in breach of the DPA. Any breach by a party of the provisions of the DPA in relation to the Processing of the Personal Data or of any other obligation of that party pursuant to the DPA shall entitle the other party to terminate any Existing Contract.
 - n) immediately notify Education Development Trust and it shall provide Education Development Trust with full co-operation and assistance in relation to any complaint, notice or communication it receives which relates directly or indirectly to the Processing of the Personal Data or to either party's compliance with the DPA.
- 4.4 The **Data Recipient** shall appoint a data protection officer, if this is legally required and, upon request of Education Development Trust, **Data Recipient** shall notify to Education Development Trust the contact details of the data protection officer.
- 4.5 **Data Recipient** shall, without undue delay, inform Education Development Trust in case of a serious interruption of operations or violations by the **Data Recipient** or persons employed by it of provisions to protect Personal Data or of terms specified in this DPA. In such an event, **Data Recipient** shall implement the measures necessary to secure the Personal Data and to mitigate potential adverse effects on the data subjects and shall agree upon the same with Education Development Trust without undue delay. **Data Recipient** shall support Education Development Trust in fulfilling Education Development Trust's disclosure obligations under DPA.
- 4.6 Education Development Trust shall retain title as to any media provided to **Data Recipient** as well as any copies or reproductions thereof. **Data Recipient** shall store such media safely and protect them against unauthorised access by third parties. **Data Recipient** shall, upon Education Development Trust's request, provide to Education Development Trust all information on Education Development Trust's Personal Data and information. **Data Recipient** shall be obliged to securely delete any test and scrap material based on an Instruction issued by Education Development Trust on a case-by-case basis. Where Education Development Trust so decides, **Data Recipient** shall hand over such material to Education Development Trust or store it on Education Development Trust's behalf.
-

- 4.7 **Data Recipient** shall be obliged to verify the fulfilment of the above-entitled obligations and shall maintain an adequate documentation of such verification.

5. OBLIGATIONS OF EDUCATION DEVELOPMENT TRUST

- 5.1 Education Development Trust and **Data Recipient** shall be separately responsible for conforming with such statutory data protection regulations as are applicable to them.
- 5.2 Education Development Trust shall inform **Data Recipient** without undue delay and comprehensively about any errors or irregularities related to statutory provisions on the Processing of Personal Data detected during a verification of the results of such Processing.
- 5.3 Education Development Trust shall be responsible for fulfilling the duties to inform individuals of the processing of their data resulting from DPA.
- 5.4 Education Development Trust shall, upon termination or expiration of the Existing Contract and by way of issuing an Instruction, stipulate, within a period of time set by **Data Recipient**, the reasonable measures by which **Data Recipient must return or delete** stored data.
- 5.5 Education Development Trust warrants that:
- (a) it has the right to license the Processing of the Personal Data for the Purpose;
 - (b) it is not aware of any circumstances likely to give rise to breach of any of the Privacy and Data Protection Requirements in the future (including any Security Breach);
 - (c) the Data Recipient is entitled to Process the Personal Data for the Purpose and such use will comply with all Privacy and Data Protection Requirements;
 - (d) all data subjects relating to the Personal Data have given their valid consent and, where required under the Privacy and Data Protection Requirements, their explicit consent to the transfer of their personal data by Education Development Trust to the Data Recipient and to the Processing of their personal data by the Data Recipient for the Purpose within England and Wales;
 - (e) all Personal Data is necessary, accurate and up-to-date; and
 - (f) it is registered with all relevant data protection authorities to Process all Personal Data for the Purpose.

6. ENQUIRIES BY DATA SUBJECTES TO EDUCATION DEVELOPMENT TRUST

- 6.1 Where Education Development Trust, based upon applicable data protection law under the DPA, is obliged to provide information to an individual about the collection, processing or use of its Personal Data, **Data Recipient** shall assist Education Development Trust in making this information available, provided that Education Development Trust has instructed **Data Recipient** in writing to do so.

- 6.2 Where a data subject requests the **Data Recipient** to correct, delete or block Personal Data, Processor shall refer such data subject to Education Development Trust as the Controller of the Data.

7. AUDIT OBLIGATIONS

- 7.1 Education Development Trust may, prior to the commencement of Processing, and at regular intervals thereafter, audit the technical and organisational measures taken by **Data Recipient**, and may document the resulting findings.
- 7.2 **Data Recipient** shall, upon Education Development Trust's written request and within a reasonable period of time, provide Education Development Trust with reasonable assistance required for such audit, in order for Education Development Trust to demonstrate compliance with the Data Protection Act 2018 / GDPR, and to allow Education Development Trust to inspect the Data Recipient's compliance.

8. SUBCONTRACTORS

- 8.1 **Data Recipient** shall be entitled to subcontract **Data Recipient's** obligations defined in the Existing Contract (insofar as they relate to the Processing of Personal Data) to third parties only with Education Development Trust's written consent.
- 8.2 Education Development Trust consents to **Data Recipient** subcontracting to **Data Recipient's subsidiaries or group** affiliated companies and any third parties that are listed in the Schedule, of **Data Recipient's** contractual obligations hereunder.
- 8.3 If the **Data Recipient** intends to instruct subcontractors other than the companies listed in the Schedule, the **Data Recipient** must notify Education Development Trust thereof in writing and request Education Development Trust's consent which shall not be unreasonably withheld.
- 8.4 Where **Data Recipient** engages subcontractors, **Data Recipient** shall be obliged to ensure that the subcontractor agrees to be bound by all **Data Recipient's** contractual obligations hereunder and Education Development Trust shall have the right to enforce any such agreement against the subcontractor.
- 8.5 The provisions of this clause shall apply where **Data Recipient engages** a subcontractor in a third country outside the EEA. Education Development Trust hereby authorizes **Data Recipient**, to agree in the name and on behalf of the Education Development Trust with a subcontractor which processes or uses Personal Data of the Education Development Trust outside of the EEA, to enter into EU Standard Contractual Clauses for the Transfer of Personal Data to Processors Established in Third Countries dated 5 February 2010 or as updated or amended. This applies accordingly from the date of this authorization with respect to EU Standard Contractual Clauses (Processors) already concluded by the **Data Recipient** with such subcontractors.

9. DUTIES TO INFORM, MANDATORY WRITTEN FORM, CHOICE OF LAW, ADDITIONAL TERMS

- 9.1 Where Education Development Trust's Personal Data becomes subject to search and seizure, an attachment order, confiscation during bankruptcy or insolvency proceedings, or similar events or measures by third parties while being Processed, **Data Recipient** shall inform Education Development Trust without undue delay. **Data Recipient** shall, without undue delay, notify to all pertinent parties in such action, that any Personal Data affected thereby is in Education Development Trust's sole property and area of responsibility, that Personal Data is at Education Development Trust's sole disposition, and that Education Development Trust is the responsible body in the sense of the DPA.
- 9.2 In case of any conflict, the provisions of this agreement shall take precedence over the provisions of the Existing Contract. Where individual clauses of this agreement are invalid or unenforceable, the validity and enforceability of the other regulations of this agreement shall not be affected.

10. LIABILITY

- 10.1 Neither party excludes or limits liability to the other party for:
- (a) fraud or fraudulent misrepresentation;
 - (b) death or personal injury caused by negligence; or
 - (c) any matter for which it would be unlawful for the parties to exclude liability.
- 10.2 Neither party, whether in contract, tort (including negligence) or otherwise (including under any indemnity under this Agreement)), and whether in connection with this agreement or any collateral contract, shall in any circumstances have any liability for any losses or damages which may be suffered by the other, which fall within any of the following categories:
- (a) any indirect or consequential losses;
 - (b) loss of profits business opportunity and management time (whether direct, indirect or consequential); or
 - (c) loss of goodwill (whether direct, indirect or consequential).
- 10.3 The Data Recipient shall indemnify and hold Education Development Trust harmless from all claims and all liabilities, costs, proceedings, damages and expenses (including legal and other professional fees and expenses) awarded against, or incurred or paid by, Education Development Trust as a result of or in connection with any alleged or actual breaches of the DPA by the Data Recipient.
- 10.4 The provisions of this clause shall survive termination of this agreement, however arising.

11. TERM AND TERMINATION

11.1 Subject to any provisions of any Existing Contract, Education Development Trust may terminate this agreement by giving four (4) weeks' written notice to the Data Recipient.

Signed:
Education Development Trust
Dated:

Signed:
Data Recipient
Dated:

Schedule

Summary of the subject-matter of the data	Data required to be processed by the Data Recipient under the Existing Contract and as set out therein
Length of time that the processing will continue	For the term of the Existing Contract
Nature and purpose of the processing	For the purposes as set out in the Existing Contract
Type(s) of personal data that will be processed	The types of Personal Data required to be processed by the Data Recipient under the Existing Contract and as set out therein
Categories of data subjects whose personal data will be processed	The categories of Personal Data required to be processed by the Data Recipient under the Existing Contract and as set out therein
Subcontractors or other companies to whom the Data Recipient may provide the Personal Data	

Schedule 4: Contract for Overseas Transfers

Introduction

For any overseas subsidiary of our company, we will have in place the Standard Contract for Processing Outside the EEA at Schedule 4. These incorporate the EU's Model Clauses to cover the transfer of personal data, and they will have copies of our policies so as to understand the levels of protection we expect.

We will monitor the creation of any new overseas subsidiary and ensure that, if and to the extent that they are conducting any processing activities in the UK, they comply with Education Development Trust's data protection policies.

It is Education Development Trust's requirement that we do not send any data outside the EEA without first considering whether we have consent to do so. If we do not have consent to such a transfer, then we will avoid sending any data outside the EEA unless it is necessary in performance of a contract, required for legal action, or it is in the public interest or the vital interests of the data subject. The decision will be taken by the Data Protection Lead for the business area or unit, in consultation where necessary with the Data Protection Officer.

If any organisation to whom Education Development Trust intends to send personal data is based outside the EEA, or intends to transfer the personal data outside the EEA, then Education Development Trust will not transfer any personal data to that organisation without first putting in place the Standard Contract for Processing Outside the EEA.

Contract for Overseas Transfers



EUROPEAN COMMISSION
DIRECTORATE-GENERAL JUSTICE

Directorate C: Fundamental rights and Union citizenship
Unit C.3: Data protection

Commission Decision C(2010)593 Standard Contractual Clauses (processors)

For the purposes of Article 26(2) of Directive 95/46/EC for the transfer of personal data to processors established in third countries which do not ensure an adequate level of data protection

Name of the data exporting organisation: Education Development Trust

Address: Highbridge House, 16-18 Duke Street, Reading, RG1 4RU

(the data **exporter**)

And

Name of the data importing organisation:.....

Address:

Tel:.....; fax:.....; e-mail:

Other information needed to identify the organisation:

.....
(the data **importer**)

each a “party”; together “the parties”,

HAVE AGREED on the following Contractual Clauses (the Clauses) in order to adduce adequate safeguards with respect to the protection of privacy and fundamental rights and freedoms of individuals for the transfer by the data exporter to the data importer of the personal data specified in Appendix 1.

Clause 1

Definitions

For the purposes of the Clauses:

- (a) *'personal data', 'special categories of data', 'process/processing', 'controller', 'processor', 'data subject' and 'supervisory authority'* shall have the same meaning as in Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data¹;
- (b) *'the data exporter'* means the controller who transfers the personal data;
- (c) *'the data importer'* means the processor who agrees to receive from the data exporter personal data intended for processing on his behalf after the transfer in accordance with his instructions and the terms of the Clauses and who is not subject to a third country's system ensuring adequate protection within the meaning of Article 25(1) of Directive 95/46/EC;
- (d) *'the subprocessor'* means any processor engaged by the data importer or by any other subprocessor of the data importer who agrees to receive from the data importer or from any other subprocessor of the data importer personal data exclusively intended for processing activities to be carried out on behalf of the data exporter after the transfer in accordance with his instructions, the terms of the Clauses and the terms of the written subcontract;
- (e) *'the applicable data protection law'* means the legislation protecting the fundamental rights and freedoms of individuals and, in particular, their right to privacy with respect to the processing of personal data applicable to a data controller in the Member State in which the data exporter is established;
- (f) *'technical and organisational security measures'* means those measures aimed at protecting personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorised disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing.

Clause 2

Details of the transfer

The details of the transfer and in particular the special categories of personal data where applicable are specified in Appendix 1 which forms an integral part of the Clauses.

¹ Parties may reproduce definitions and meanings contained in Directive 95/46/EC within this Clause if they considered it better for the contract to stand alone.

Clause 3

Third-party beneficiary clause

1. The data subject can enforce against the data exporter this Clause, Clause 4(b) to (i), Clause 5(a) to (e), and (g) to (j), Clause 6(1) and (2), Clause 7, Clause 8(2), and Clauses 9 to 12 as third-party beneficiary.
2. The data subject can enforce against the data importer this Clause, Clause 5(a) to (e) and (g), Clause 6, Clause 7, Clause 8(2), and Clauses 9 to 12, in cases where the data exporter has factually disappeared or has ceased to exist in law unless any successor entity has assumed the entire legal obligations of the data exporter by contract or by operation of law, as a result of which it takes on the rights and obligations of the data exporter, in which case the data subject can enforce them against such entity.
3. The data subject can enforce against the subprocessor this Clause, Clause 5(a) to (e) and (g), Clause 6, Clause 7, Clause 8(2), and Clauses 9 to 12, in cases where both the data exporter and the data importer have factually disappeared or ceased to exist in law or have become insolvent, unless any successor entity has assumed the entire legal obligations of the data exporter by contract or by operation of law as a result of which it takes on the rights and obligations of the data exporter, in which case the data subject can enforce them against such entity. Such third-party liability of the subprocessor shall be limited to its own processing operations under the Clauses.
4. The parties do not object to a data subject being represented by an association or other body if the data subject so expressly wishes and if permitted by national law.

Clause 4

Obligations of the data exporter

The data exporter agrees and warrants:

- (a) that the processing, including the transfer itself, of the personal data has been and will continue to be carried out in accordance with the relevant provisions of the applicable data protection law (and, where applicable, has been notified to the relevant authorities of the Member State where the data exporter is established) and does not violate the relevant provisions of that State;
- (b) that it has instructed and throughout the duration of the personal data processing services will instruct the data importer to process the personal data transferred only on the data exporter's behalf and in accordance with the applicable data protection law and the Clauses;
- (c) that the data importer will provide sufficient guarantees in respect of the technical and organisational security measures specified in Appendix 2 to this contract;
- (d) that after assessment of the requirements of the applicable data protection law, the security measures are appropriate to protect personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorised disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing, and that these measures ensure a level of security appropriate to the risks presented by the processing and the nature of the data to be protected having regard to the state of the art and the cost of their implementation;

- (e) that it will ensure compliance with the security measures;
- (f) that, if the transfer involves special categories of data, the data subject has been informed or will be informed before, or as soon as possible after, the transfer that its data could be transmitted to a third country not providing adequate protection within the meaning of Directive 95/46/EC;
- (g) to forward any notification received from the data importer or any subprocessor pursuant to Clause 5(b) and Clause 8(3) to the data protection supervisory authority if the data exporter decides to continue the transfer or to lift the suspension;
- (h) to make available to the data subjects upon request a copy of the Clauses, with the exception of Appendix 2, and a summary description of the security measures, as well as a copy of any contract for subprocessing services which has to be made in accordance with the Clauses, unless the Clauses or the contract contain commercial information, in which case it may remove such commercial information;
- (i) that, in the event of subprocessing, the processing activity is carried out in accordance with Clause 11 by a subprocessor providing at least the same level of protection for the personal data and the rights of data subject as the data importer under the Clauses; and
- (j) that it will ensure compliance with Clause 4(a) to (i).

Clause 5

Obligations of the data importer²

The data importer agrees and warrants:

- (a) to process the personal data only on behalf of the data exporter and in compliance with its instructions and the Clauses; if it cannot provide such compliance for whatever reasons, it agrees to inform promptly the data exporter of its inability to comply, in which case the data exporter is entitled to suspend the transfer of data and/or terminate the contract;
- (b) that it has no reason to believe that the legislation applicable to it prevents it from fulfilling the instructions received from the data exporter and its obligations under the contract and that in the event of a change in this legislation which is likely to have a substantial adverse effect on the warranties and obligations provided by the Clauses, it will promptly notify the change to the data exporter as soon as it is aware, in which case the data exporter is entitled to suspend the transfer of data and/or terminate the contract;
- (c) that it has implemented the technical and organisational security measures specified in Appendix 2 before processing the personal data transferred;
- (d) that it will promptly notify the data exporter about:

² Mandatory requirements of the national legislation applicable to the data importer which do not go beyond what is necessary in a democratic society on the basis of one of the interests listed in Article 13(1) of Directive 95/46/EC, that is, if they constitute a necessary measure to safeguard national security, defence, public security, the prevention, investigation, detection and prosecution of criminal offences or of breaches of ethics for the regulated professions, an important economic or financial interest of the State or the protection of the data subject or the rights and freedoms of others, are not in contradiction with the standard contractual clauses. Some examples of such mandatory requirements which do not go beyond what is necessary in a democratic society are, *inter alia*, internationally recognised sanctions, tax-reporting requirements or anti-money-laundering reporting requirements.

- (i) any legally binding request for disclosure of the personal data by a law enforcement authority unless otherwise prohibited, such as a prohibition under criminal law to preserve the confidentiality of a law enforcement investigation,
 - (ii) any accidental or unauthorised access, and
 - (iii) any request received directly from the data subjects without responding to that request, unless it has been otherwise authorised to do so;
- (e) to deal promptly and properly with all inquiries from the data exporter relating to its processing of the personal data subject to the transfer and to abide by the advice of the supervisory authority with regard to the processing of the data transferred;
- (f) at the request of the data exporter to submit its data processing facilities for audit of the processing activities covered by the Clauses which shall be carried out by the data exporter or an inspection body composed of independent members and in possession of the required professional qualifications bound by a duty of confidentiality, selected by the data exporter, where applicable, in agreement with the supervisory authority;
- (g) to make available to the data subject upon request a copy of the Clauses, or any existing contract for subprocessing, unless the Clauses or contract contain commercial information, in which case it may remove such commercial information, with the exception of Appendix 2 which shall be replaced by a summary description of the security measures in those cases where the data subject is unable to obtain a copy from the data exporter;
- (h) that, in the event of subprocessing, it has previously informed the data exporter and obtained its prior written consent;
- (i) that the processing services by the subprocessor will be carried out in accordance with Clause 11;
- (j) to send promptly a copy of any subprocessor agreement it concludes under the Clauses to the data exporter.

Clause 6

Liability

1. The parties agree that any data subject, who has suffered damage as a result of any breach of the obligations referred to in Clause 3 or in Clause 11 by any party or subprocessor is entitled to receive compensation from the data exporter for the damage suffered.
2. If a data subject is not able to bring a claim for compensation in accordance with paragraph 1 against the data exporter, arising out of a breach by the data importer or his subprocessor of any of their obligations referred to in Clause 3 or in Clause 11, because the data exporter has factually disappeared or ceased to exist in law or has become insolvent, the data importer agrees that the data subject may issue a claim against the data importer as if it were the data exporter, unless any successor entity has assumed the entire legal obligations of the data exporter by contract or by operation of law, in which case the data subject can enforce its rights against such entity.

The data importer may not rely on a breach by a subprocessor of its obligations in order to avoid its own liabilities.
3. If a data subject is not able to bring a claim against the data exporter or the data importer referred to in paragraphs 1 and 2, arising out of a breach by the subprocessor of any of

their obligations referred to in Clause 3 or in Clause 11 because both the data exporter and the data importer have factually disappeared or ceased to exist in law or have become insolvent, the subprocessor agrees that the data subject may issue a claim against the data subprocessor with regard to its own processing operations under the Clauses as if it were the data exporter or the data importer, unless any successor entity has assumed the entire legal obligations of the data exporter or data importer by contract or by operation of law, in which case the data subject can enforce its rights against such entity. The liability of the subprocessor shall be limited to its own processing operations under the Clauses.

Clause 7

Mediation and jurisdiction

1. The data importer agrees that if the data subject invokes against it third-party beneficiary rights and/or claims compensation for damages under the Clauses, the data importer will accept the decision of the data subject:
 - (a) to refer the dispute to mediation, by an independent person or, where applicable, by the supervisory authority;
 - (b) to refer the dispute to the courts in the Member State in which the data exporter is established.
2. The parties agree that the choice made by the data subject will not prejudice its substantive or procedural rights to seek remedies in accordance with other provisions of national or international law.

Clause 8

Cooperation with supervisory authorities

1. The data exporter agrees to deposit a copy of this contract with the supervisory authority if it so requests or if such deposit is required under the applicable data protection law.
2. The parties agree that the supervisory authority has the right to conduct an audit of the data importer, and of any subprocessor, which has the same scope and is subject to the same conditions as would apply to an audit of the data exporter under the applicable data protection law.
3. The data importer shall promptly inform the data exporter about the existence of legislation applicable to it or any subprocessor preventing the conduct of an audit of the data importer, or any subprocessor, pursuant to paragraph 2. In such a case the data exporter shall be entitled to take the measures foreseen in Clause 5 (b).

Clause 9

Governing Law

The Clauses shall be governed by the law of the Member State in which the data exporter is established, namely the United Kingdom of Great Britain and Northern Ireland

Clause 10

Variation of the contract

The parties undertake not to vary or modify the Clauses. This does not preclude the parties from adding clauses on business related issues where required as long as they do not contradict the Clause.

Clause 11

Subprocessing

1. The data importer shall not subcontract any of its processing operations performed on behalf of the data exporter under the Clauses without the prior written consent of the data exporter. Where the data importer subcontracts its obligations under the Clauses, with the consent of the data exporter, it shall do so only by way of a written agreement with the subprocessor which imposes the same obligations on the subprocessor as are imposed on the data importer under the Clauses³. Where the subprocessor fails to fulfil its data protection obligations under such written agreement the data importer shall remain fully liable to the data exporter for the performance of the subprocessor's obligations under such agreement.
2. The prior written contract between the data importer and the subprocessor shall also provide for a third-party beneficiary clause as laid down in Clause 3 for cases where the data subject is not able to bring the claim for compensation referred to in paragraph 1 of Clause 6 against the data exporter or the data importer because they have factually disappeared or have ceased to exist in law or have become insolvent and no successor entity has assumed the entire legal obligations of the data exporter or data importer by contract or by operation of law. Such third-party liability of the subprocessor shall be limited to its own processing operations under the Clauses.
3. The provisions relating to data protection aspects for subprocessing of the contract referred to in paragraph 1 shall be governed by the law of the Member State in which the data exporter is established, namely
.....
.....
4. The data exporter shall keep a list of subprocessing agreements concluded under the Clauses and notified by the data importer pursuant to Clause 5 (j), which shall be updated at least once a year. The list shall be available to the data exporter's data protection supervisory authority.

Clause 12

Obligation after the termination of personal data processing services

1. The parties agree that on the termination of the provision of data processing services, the data importer and the subprocessor shall, at the choice of the data exporter, return all the personal data transferred and the copies thereof to the data exporter or shall destroy all

³ This requirement may be satisfied by the subprocessor co-signing the contract entered into between the data exporter and the data importer under this Decision.

the personal data and certify to the data exporter that it has done so, unless legislation imposed upon the data importer prevents it from returning or destroying all or part of the personal data transferred. In that case, the data importer warrants that it will guarantee the confidentiality of the personal data transferred and will not actively process the personal data transferred anymore.

2. The data importer and the subprocessor warrant that upon request of the data exporter and/or of the supervisory authority, it will submit its data processing facilities for an audit of the measures referred to in paragraph 1.

On behalf of the data exporter:

Name (written out in full):

Position:

Address:

Other information necessary in order for the contract to be binding (if any):

Signature.....

(stamp of organisation)

On behalf of the data importer:

Name (written out in full):

Position:

Address:

Other information necessary in order for the contract to be binding (if any):

Signature.....

(stamp of organisation)

APPENDIX 1 TO THE STANDARD CONTRACTUAL CLAUSES

This Appendix forms part of the Clauses and must be completed and signed by the parties. The Member States may complete or specify, according to their national procedures, any additional necessary information to be contained in this Appendix.

Data exporter

The data exporter is (please specify briefly your activities relevant to the transfer):

.....
.....

Data importer

The data importer is (please specify briefly activities relevant to the transfer):

.....
.....

Data subjects

The personal data transferred concern the following categories of data subjects (please specify):

.....
.....

Categories of data

The personal data transferred concern the following categories of data (please specify):

.....
.....

Special categories of data (if appropriate)

The personal data transferred concern the following special categories of data (please specify):

.....
.....

Processing operations

The personal data transferred will be subject to the following basic processing activities (please specify):

.....
.....

DATA EXPORTER

Name:.....

Authorised Signature

DATA IMPORTER

Name:.....

Authorised Signature

APPENDIX 2 TO THE STANDARD CONTRACTUAL CLAUSES

This Appendix forms part of the Clauses and must be completed and signed by the parties.
Description of the technical and organisational security measures implemented by the data importer in accordance with Clauses 4(d) and 5(c) (or document/legislation attached):

.....
.....
.....
.....
.....

ILLUSTRATIVE INDEMNIFICATION CLAUSE (OPTIONAL)

Liability

The parties agree that if one party is held liable for a violation of the clauses committed by the other party, the latter will, to the extent to which it is liable, indemnify the first party for any cost, charge, damages, expenses or loss it has incurred.

Indemnification is contingent upon:

- (a) the data exporter promptly notifying the data importer of a claim; and
- (b) the data importer being given the possibility to cooperate with the data exporter in the defence and settlement of the claim⁴.

⁴ Paragraph on liabilities is optional.

Schedule 5: Data Protection Impact Assessment

Introduction

Data Protection Impact Assessments will be carried out for every new external project and all internal projects where personal data will be required, in order to assess the likely effect of any data collected as part of the project on the individuals from whom it is collected and whether it is necessary or appropriate to do so in the proposed manner. Ideas for minimising risk to those individuals (through data security breaches or otherwise) will be considered and then implemented as part of the project design.

If a Data Impact Assessment determines that there would be an unacceptable level of impact on individuals, alternatives will be considered up to and including not proceeding with the project.

Data Impact Assessments will be kept with project or activity related documentation and retained for as long as that documentation (contracts, bids, personnel records) is kept.

We will also implement data protection impact assessments for any other high risk processing i.e. automated processing including profiling that produce legal effects or similarly significantly affect individuals; any processing of sensitive personal data (including children's data, Biometric and photographic data); and systematic monitoring of publicly accessible areas on a large scale.

Data Protection Impact Assessment Form

Name of Project/Activity:

Personal data that might be collected or used:

- e.g.
1. *names*
 2. *addresses*
 3. *history of work within the region*
 4. *religion*

For each piece of data that might be collected:

How necessary is it that we collect it?

- e.g.
1. *name – vital, cannot work without it*
 2. *address – vital, client insists that we keep it*
 3. *history of work within the region – useful, to assess conflicts of interest and compliance*
 4. *religion – potentially useful, to assess potential cultural considerations/risks*

How necessary is it that we keep it and for how long?

- e.g.
1. *name – until there is no longer any chance of needing to prove or refer to the individual's involvement.*
 2. *address – until there is no longer any chance of needing to contact the individual*
 3. *history of work within the region – until the compliance process for that individual is complete*

4. religion – until the potential cultural considerations/risks have been assessed and mitigated

Can it be minimised or made anonymous?

Is automated decision making going to be used? If so, is it really necessary and can the automated decisions be manually checked?

Is it going to be passed on to any other organisations (and if so, what arrangements are there in place to make sure that any transfer is secure)?

What risk is there to any individual due to the collection and storage or use of that data?

What risk would there be to any individual should the data be lost or disclosed to third parties?

What management or mitigation measures should be put in place to minimise those risks (especially, not collecting so much data if possible, a clear deletion process at close-down or simply not storing it in the first place)?

Legitimate Interests (if we are unable to implement a process for obtaining consent)

Does the business have a legitimate need to process this data irrespective of the consent of the individuals?

Is there any other way to protect those interests which are less intrusive of individual data rights?

Are we justified in considering the identified legitimate interests to outweigh the impact on individuals identified above (and that we are not using the data in a way that is intrusive, harmful or different to how they would reasonably expect it to be used)?

Could we offer a safeguard or an opt-out?

In light of the above, is it appropriate to collect and use the data?

Schedule 6: Record of Processing Activities: Education Development Trust

Controller: Education Development Trust

Nature of work – Education Charity

Reasons/purposes for processing information

We process personal information to enable us to achieve our charitable objectives in the field of education, in accordance with our Articles of Association. In particular we use personal data to provide education and training to our customers and clients; to promote and provide our services, to maintain our own accounts and records and to support and manage our employees. We also use CCTV for security and the prevention and detection of crime.

We also use it for administering any accounts; processing bank details for payment purposes; the prevention or detection of fraud; market research; marketing; Disclosure and Barring Service checks; credit reference checks

Type/classes of information processed

We process information relevant to the above reasons/purposes. This may include:

- personal details
- family details
- business activities of the person whose personal information we are processing
- lifestyle and social circumstances
- financial details
- training details
- education and employment details
- goods and services
- visual images, personal appearance and behaviour

We also process sensitive classes of information that may include:

- physical or mental health details
- racial or ethnic origin
- religious or other beliefs
- trade union membership

Who the information is processed about

We process personal information about:

- customers
 - clients
 - students
 - trainers
 - employees
-

- suppliers
- professional advisers and consultants
- complainants, enquirers
- individuals captured by CCTV images
- contractors and subcontractors
- consultants and partner organisations

Who the information may be shared with

We sometimes need to share the personal information we process with other organisations with whom we work to deliver the activities described under the paragraph “Reasons/purposes for processing information”. What follows is a description of the types of organisations we may need to share some of the personal information we process with for one or more reasons. Business associates, clients, local authorities, charities; professional advisers; educators and examining bodies; current, past or prospective employers; family, associates and representatives of the person whose personal data we are processing; employment and recruitment agencies; financial organisations; credit reference agencies; debt collection and tracing agencies; suppliers and service providers; persons making an enquiry or complaint; other companies in the same group; central government; police forces, courts

Undertaking Research

Personal information is also processed in order to undertake research. For this reason, the information processed may include name, contact details, family details, lifestyle and social circumstances, financial details, goods and services. The sensitive types of information may include physical or mental health details, racial or ethnic origin and religious or other beliefs. This information is about survey respondents. Where necessary or required this information may be shared with customers and clients, agents, service providers, survey and research organisations.

Transfers

It may sometimes be necessary to transfer personal information overseas. When this is needed information may be transferred to countries or territories around the world.

Record of Processing Activities: Schools

Controller: [name of school]

Nature of work – Education provider

Reasons/purposes for processing information

We process personal information to enable us to achieve our educational objectives, in accordance with our proprietor Education Development Trust's Articles of Association. In particular we use personal data to provide education to our pupils and administrative services to our staff; to promote and provide our services, to maintain our own accounts and records and to support and manage our employees. We may also use CCTV for security and the prevention and detection of crime.

We also use personal data for processing bank details for payment purposes; the prevention or detection of fraud; market research; marketing; Disclosure and Barring Service checks; credit reference checks.

Type/classes of information processed

We process information relevant to the above reasons/purposes. This may include:

- personal details
- family details
- business activities of the person whose personal information we are processing
- lifestyle and social circumstances
- financial details
- training details
- education and employment details
- goods and services
- visual images, personal appearance and behaviour

We also process sensitive classes of information that may include:

- data of children under 16 years of age
- physical or mental health details
- racial or ethnic origin
- religious or other beliefs
- trade union membership

Who the information is processed about

We process personal information about:

- parents of pupils
- service providers
- students

- trainers
- employees
- suppliers
- professional advisers and consultants
- complainants, enquirers
- individuals captured by CCTV images
- contractors and subcontractors
- consultants and partner organisations

Who the information may be shared with

We sometimes need to share the personal information we process with other organisations with whom we work to deliver the activities described under the paragraph “Reasons/purposes for processing information”. What follows is a description of the types of organisations we may need to share some of the personal information we process with for one or more reasons.

Our proprietor, Education Development Trust; Business associates, clients, local authorities, charities; professional advisers; educators and examining bodies; current, past or prospective employers; family, associates and representatives of the person whose personal data we are processing; employment and recruitment agencies; financial organisations; credit reference agencies; debt collection and tracing agencies; suppliers and service providers; persons making an enquiry or complaint; other companies in the same group; central government; police forces, courts

Undertaking Research

Personal information is also processed in order to undertake research. For this reason the information processed may include name, contact details, family details, lifestyle and social circumstances, financial details, good and services. The sensitive types of information may include physical or mental health details, racial or ethnic origin and religious or other beliefs. This information is about survey respondents. Where necessary or required this information may be shared with customers and clients, agents, service providers, survey and research organisations.

Transfers

It may sometimes be necessary to transfer personal information overseas. When this is needed information may be transferred to countries or territories around the world.

Schedule 7: Website Privacy Notice

NB: THIS MUST BE USED AS A SEPARATE NOTICE AND NOT SIMPLY ADDED TO THE WEBSITE TERMS AND CONDITIONS, DISCLAIMER AND COPYRIGHT NOTICE

The General Data Protection Regulation 2017 requires Education Development Trust to provide you with certain information when you have provided it with personal data.

'Personal data' means information relating to an identified or identifiable living person.

The Privacy Notice, which incorporates the Standard Data Collection Form, sets out how Education Development Trust uses and protects any information that you give Education Development Trust when you use this website. It will be accessible on our websites, and (including project specific websites) will first require individuals to indicate their agreement to the Notice, whether through a tick box or other means. Any such tick box will require a positive tick to say, "I agree" and will not utilise a pre-ticked box or "opt out".

Education Development Trust is committed to ensuring that your privacy is protected. Should we ask you to provide certain information by which you can be identified when using this website, then you can be assured that it will only be used in accordance with this privacy statement.

Education Development Trust may change this policy from time to time by updating this page. You should check this page from time to time to ensure that you are happy with any changes. This policy is effective from [date].

Who are we?

Education Development Trust is a registered charity and company limited by guarantee, incorporated in England and Wales. It is a 'controller' under the General Data Protection Regulation. Occasionally it will also act as a 'processor' and if we are acting as a processor then the controller will be listed below or provided to you orally or through email at the time of collection of the data:

Controller: _____

What we collect

We will only collect information from you that is relevant to the circumstances in which we are working with you. In particular, we may collect the following information from you which is defined as 'personal data':

- Name, date of birth and job title
- contact information including email address
- demographic information such as postcode, preferences and interests
- other information relevant to services

How we use your Information

We require this information to understand your needs and provide you with a better service, and in particular for the following reasons:

- Internal record keeping.

- Transfer of data to third parties, for example under contracts with the website host or operator, or any government department or organisation for whom the website was designed, which may include a transfer outside of the EEA
- We may use the information to improve our products, materials and services.
- We may periodically send promotional emails about new products, special offers or other information which we think you may find interesting using the email address which you have provided.
- From time to time, we may also use your information to contact you for market research purposes. We may contact you by email, phone, fax or mail. We may use the information to customise the website according to your interests.

Security

We are committed to ensuring that your information is secure. In order to prevent unauthorised access or disclosure, we have put in place suitable physical, technical, electronic and managerial procedures to safeguard and secure the information we collect online. Information will not be held for longer than it is needed.

Who will we share your information with?

We sometimes need to share the personal information we process with other organisations with whom we work to deliver the activities described under the paragraph "*How we use your information*" What follows is a description of the types of organisations we may need to share some of the personal information we process with for one or more reasons:

[...]

For how long will we keep your information?

We will keep your information throughout the period of time that we work with you and for the duration of any project or association with us as part of which you provided the personal data, and for a period of six years from that point or until it is no longer necessary for us to hold the data.

Will my data be transferred outside the European Economic Area?

Our data servers or those which host our software are or may be located in the United States and so your data is likely to be transferred outside the EEA under contractual arrangements with the relevant companies providing those servers or hosting services. If you have provided data to us as part of a project that is being delivered by or with or that is linked to any of our overseas offices, then we may also need to transfer your data outside the EEA.

What rights do you have?

You have a series of rights under the General Data Protection Regulation including the right to access a copy of the information we hold about you, to have data we hold erased, to restrict the use of your data, to object to marketing use of your data, the right to withdraw consent to our processing of your data, rights concerning the portability of your data. Further information on this issue can be obtained from our Data Protection Officer at sclifton@educationdevelopmenttrust.com

In particular, you may choose to restrict the collection or use of your personal information in the following ways:

- whenever you are asked to fill in a form on the website, look for the box that you can click to indicate that you do not want the information to be used by anybody for direct marketing purposes
- if you have previously agreed to us using your personal information for direct marketing purposes, you may change your mind at any time by writing to or emailing us at [email address]

We will not sell, distribute or lease your personal information to third parties unless we have your permission or are required or entitled by law to do so. We may use your personal information to send you promotional information about third parties which we think you may find interesting if you tell us that you wish this to happen.

You may request details of personal information which we hold about you under the Data Protection Act 2018. If you would like a copy of the information held on you please write to our head office address.

If you believe that any information we are holding on you is incorrect or incomplete, please write to or email us as soon as possible at the above address. We will promptly correct any information found to be incorrect.

Who can you complain to if you are unhappy about what we have done with your information?

If you are unhappy about how we are using your information then initially you should contact the Data Protection Officer and if your complaint remains unresolved then you can contact the Information Commissioner's Office, details available at www.ico.org.uk.

Marketing

I am happy for my personal data to be used for the purposes of direct marketing of Education Development Trust's services.

Cookies

A cookie is a small file which asks permission to be placed on your computer's hard drive. Once you agree, the file is added and the cookie helps analyse web traffic or lets you know when you visit a particular site. Cookies allow web applications to respond to you as an individual. The web application can tailor its operations to your needs, likes and dislikes by gathering and remembering information about your preferences.

The only cookies in use on this website are for [e.g. Google Analytics]. [Google Analytics] is a web analytics tool that helps website owners understand how visitors engage with their website. [Google Analytics] customers can view a variety of reports about how visitors interact with their website so that they can improve it. [Google Analytics] collects information anonymously. It reports website trends without identifying individual visitors.

You can opt out of [Google Analytics] without affecting how you visit our site – for more information on opting out of being tracked by [Google Analytics] across all websites you use, visit this [Google] page. We use traffic log cookies to identify which pages are being used. This

helps us analyse data about webpage traffic and improve our website in order to tailor it to customer needs. We only use this information for statistical analysis purposes and then the data is removed from the system.

Overall, cookies help us provide you with a better website by enabling us to monitor which pages you find useful and which you do not. A cookie in no way gives us access to your computer or any information about you, other than the data you choose to share with us.

You can choose to accept or decline cookies. Most web browsers automatically accept cookies, but you can usually modify your browser setting to decline cookies if you prefer. This may prevent you from taking full advantage of the website.

Other Websites

Our website may contain links to other websites of interest. However, once you have used these links to leave our site, you should note that we do not have any control over that other website. Therefore, we cannot be responsible for the protection and privacy of any information which you provide whilst visiting such sites and such sites are not governed by this privacy statement. You should exercise caution and look at the privacy statement applicable to the website in question.

Schedule 8: Data Subject Access Request Definition and Procedure

Brief Overview of the Law

The law gives all individuals about whom Education Development Trust holds personal information the right to access information that relates to them whether it is held electronically or in manual form. A request from an individual asking for a list of the data held containing their personal data and copies of that data is known as a Data Subject Access Request (or a DSAR).

In practice, any request received from any individual about information held on them could be a DSAR even if they do not mention the law at all. Any such request received by any staff should be passed to the Data Protection Lead for guidance as to:

1. Whether it is a DSAR; and
2. If it is, how to proceed.

Generally, a data subject is entitled to request a copy of the information related to them and Education Development Trust must comply with the request within one month (no longer the 40 days under the old law) unless there is a reason under the Act not to do so or an exemption applies. Where documents are provided in response to a request, those documents will need to be reviewed and any third party's data that Education Development Trust does not have permission to disclose will need to be removed.

An initial response will be sent to the requestor within one week of receiving an access request. The response will confirm the request has been complied with, indicate the intention to comply, or give the reasons for regarding the request as unjustified. If, for any reason, these timescales cannot be met, the reason will be explained in writing to the individual making the request.

Rights of Individuals

Education Development Trust recognises the many rights that individual data subjects have under the Data Protection Act 2018 / GDPR. Any request received by an individual regarding the personal data we hold about them must be provided to the Data Protection Lead for the unit or department immediately. The Lead will then ensure it is dealt with in compliance with this policy.

All individuals on whom Education Development Trust holds data have the right to:

- Be informed upon request of all the information held about them within one month (see the part of this policy dealing with Data Subject Access Requests – this replaces the 40 days under the old law). Object to data processing relating to them which is likely to cause substantial and unwarranted damage or distress.
- Prevent the processing of their data for the purpose of direct marketing.
- Compensation if they can show that they have been caused damage by any contravention of the Act.
- The removal and correction of any inaccurate data about them.

Education Development Trust will also ensure, through the Data Protection Leads, that we commit to the principles of:

Rectification – if we are asked by someone to rectify their data, we will do so within a reasonable time and communicate to the person what measures we are taking to do so. Data

Protection Leads will ensure that such requests are dealt with quickly and that communication with the data subject is maintained.

Erasure – if someone asks for us to erase their data, we will do so as soon as reasonably practicable. Even if we are not asked to, we will do so whenever: it is no longer necessary for the purpose for which it was collected, the consent of the subject is withdrawn, the data subject objects to the processing, the data is being unlawfully processed, or we have a legal requirement to erase it. Data Protection Leads will ensure that such requests are dealt with quickly and that communication with the data subject is maintained.

Where we do erase data in response to a request from the data subject, we will inform any third parties we believe hold the same data. We will refuse to delete data where we need it to defend legal claims, to comply with legal obligations, for archive or historical purposes, in the interests of public health or other public interests, or where needed on the basis of freedom of expression.

Restriction – if a data subject wishes to restrict our processing, we will agree if its accuracy is contested or they are objecting to us deleting or processing it for a good reason (i.e. they need us to keep it or restrict it to establish or defend a claim). If we agree, we will store it but not process it, retain it only minimally, inform any third parties of the request, and if we are unable to restrict it for any reason we will inform them (so that they can ask us to erase it). Data Protection Leads will ensure that such requests are dealt with quickly and that communication with the data subject is maintained.

Portability – if someone wants their data to be passed somewhere else, where it is in a computerised form and in a machine-readable format, then we will comply. We will do so within one month of the request. However, if we do not hold it in a format that allows it to be simply provided for the use of the other organisation or service provider then we will not agree. We will also not agree if the basis for our processing of the data is on the basis of our “legitimate interests”. Data Protection Leads will ensure that such requests are dealt with quickly and that communication with the data subject is maintained.

Profiling – if a person wishes to have a decision of ours reviewed, which has been reached through automated decision making or profiling, then we will have it reviewed through human intervention unless an applicable exemption applies. Data Protection Leads will ensure that such requests are dealt with quickly and that communication with the data subject is maintained.

We will ensure that any automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to a person, in particular to analyse or predict aspects concerning their performance at work, economic situation, health, preferences, interests, reliability, behaviour location or movements, will be done only on the basis of consent or appropriate safeguards. Data Protection Leads will ensure that such requests are dealt with quickly and that communication with the data subject is maintained.

How we respond – The DSAR Procedure

The usual way to respond is:

1. The Data Protection Officer sends an initial response within a week of receiving the request. The response will confirm the request has been or is being complied with, indicate our intention to comply, and if, for any reason, the timescales cannot be met, the reason will be explained.

2. The Data Protection Officer, with support from the Data Protection Lead and their business area, conducts the search in line with what they have requested, and print everything out. The printed documents are then reviewed, and any information that is confidential to anyone else or of a commercially sensitive nature is blacked out and redacted. Any communications either sent to or from lawyers for the purposes of legal advice and any documents prepared for the purposes of litigation would be removed and not disclosed (this is “legal professional privilege” and “litigation privilege”).

3. The Data Protection Officer then provides a final response setting out what we’ve searched for, where we searched for it and the limits of the searches. That response will generally provide the data in a printed form.

Conducting the search

It is important that we can demonstrate that we’ve been thorough and careful in our search for personal data. That means we need to find ways to locate documents that contain the personal data and target the places we think it is likely to exist or where it might exist. It is not necessary to search every place that it could exist, because that would be excessive.

We also only need to search “relevant filing systems”, that is to say places where information is stored in a structured manner which can be searched. We would not be expected to rifle through loose papers in a desk drawer, for example, or retrieve rough notes that have been left in a waste paper bin or track down bits of paper that were discarded. So, we would expect to search:

- Physical filing cabinets and physical notebooks filed in a searchable manner
- Email inboxes and outboxes, including any “deleted” email folders that have not been permanently erased yet. Whilst it is possible to reconstitute permanently deleted emails, the process is both long and very expensive, and so we generally take the view that it is excessive and unreasonable to require this to be done in response to a data subject access request.
- Hard drives of work computers and laptops
- Company mobile phones of staff (for texts, emails, whatsapp messages etc)
- Administrative files holding documents about children and parents

Step One

The first step is to decide whether we know what we are looking for, where we could find it and who should look for it.

The letter from the requester should state what they want, for example:

1. All information held about the data subject.
2. the data subject’s personal school file
3. Minutes of conversations/telephone conversations with line managers
4. The data subject’s personal files

So, for each of items 2 - 4, we need to consider if there are particular places where those documents might be, and if so, assign a particular person to locate them and copy them ready for review. If we do not know what we are being asked to look for (i.e. if we do not know what a “personal visual timetable” means) then we will need to ask the requester for a clarification of that point.

However, since 1 is a request for everything, points 2 – 4 should be revealed if we hold them at all simply as a result of the general search. Every person who might have access to any documentation referring to the subject should move to step two.

Step Two

For emails (using Microsoft Outlook):

Use the Find facility to search each individual folder you have, including your inbox, sent items and deleted items folder:

- Select a folder in Outlook
- Click in the “search current mailbox” taskbar at the top of the folder
- Click on “search tools” and type the person’s surname in the ‘Search for the word(s)’ box
- Select ‘subject field and body’ from the drop down list for “In:”.
- Hit “find now”.

Outlook will display a list of the emails which contain the surname in that folder. Repeat for all other folders.

Perform a similar search on the various computer drives and devices used by the individuals searching for the information and any other locations as explained above – just searching for the person’s surname each time.

The physical documents will need to be reviewed in person, and any documents containing the surname that (are about the person*) will need to be gathered up and copied.

*A document might well have on it the person’s name, but not be “about” them. If a document refers to a person, but does not “relate” to them, could not be used to learn anything about them, is not linked to them or providing any particular information about them, is not used to inform decisions about them, has no biographical significance, and does not focus on them as a central theme, and would have no impact on them, then it is not “about” them. For example, an email might carry the subject line ‘Meeting about Tom Smith’ but if the email only contains details about whether people can attend the meeting, the email is not *about* Tom Smith.

If you are not sure about the test for what is “about” the person, then gather it and copy it. The review at step three will catch it.

Step Three

The information will need to be reviewed. Once you have collected together the information you hold, it should be sent to head office – to the Data Protection Officer - where we will examine it in detail to establish if it should be disclosed. We will also remove any data that should not be disclosed and any third party data.

If you are going to send the e-mails or documents to the Data Protection Officer for review in paper format, we would ask that you print each e-mail on a new page, single-sided, and not number the pages.

Exemptions may apply to some documents and it will be difficult to apply these exemptions if they are printed in one batch or continuously numbered. Do not staple the information and do not write comments on it; this will make it difficult to make copies to send to the requester.

If a record was created by a member of staff acting in a private rather than an official capacity, then we will not generally disclose it without their consent which may or may not be reasonable to request. If they are not prepared to disclose the record, we will not disclose it.

We will then remove data about other individuals using the following basic approach:

- If the record is primarily about the data subject, with incidental information about others, we will redact it (blank out the third party information).
- If the record is primarily about third parties and only incidentally about the data subject, we will generally withhold it if blanking out is not possible or would be excessive and of little material use to anyone.
- If the record can't be redacted but is still primarily about the data subject, we would need to contact the third party to obtain consent to disclose the document if possible.

Step Four

We would then get the documents ready to be sent to the requester.

The requester will be sent a summary in the DSAR log, of what was searched, what terms were used, and what was withheld or excluded.

Schedule 9: Data Retention

Introduction

Education Development Trust will only hold personal data for as long as necessary for the purposes for which it was collected.

Before collecting or processing personal information Education Development Trust must consider whether the information collected on staff and other data subjects is necessary for the employment or relevant contractual relationship. For example, information concerning an employee's life outside work is unlikely to be necessary. However, it might be legitimate to request information about an employee's other jobs where there is a justifiable need, for example, in connection with Working Time Regulations, or to request information about their children in connection with an application for parental leave.

Before disposing of any data Education Development Trust will consider the following key points:

- Any legal or contractual requirements;
- The length of any appeals or litigation procedure relating to the information and the time limits within which such procedures may be initiated;
- The number of times in the last two or three years that a particular type of record has been accessed.

Fundamentally though, the principle is that we will hold it only as long as it is necessary. If after a certain point the details of an identifiable person can be replaced by something more like a statistic, then the personal details are no longer needed.

As a general rule, we will hold documents containing personal data on site for as long as the data within them is considered useful for the current project or activity for which it was collected. At the point it is no longer considered useful or necessary for the current project or activity, we will consider whether to anonymise the documents in which it is held, delete it or hold the document in archive.

Where documents are to be held in archive, we will then consider whether or not we need to keep any personal data in the document or not. The table at Schedule 9 illustrates, for guidance purposes, the length of time data in those documents should be kept. This is not an exhaustive list, and the decision at each point must be made on a case by case basis, using common sense to answer the question “do we actually need to keep this personal data or not?”

The retention periods referred to in this Schedule are guidelines only and are subject to any contractual or statutory requirements concerning the retention of the specific information in question at any given time. This Schedule is not intended to be a comprehensive set of instructions to all areas of the business for holding all types of document. Business areas are expected to be familiar with their own statutory obligations as they apply to their particular function and to apply those rules.

It will be for the Data Protection Leads in each team to familiarise themselves with the rules and requirements surrounding information collected in their specific area, either from the relevant contract or the legislation in place governing their organisational/business practices.

In the absence of any contractual or statutory requirement, the test is: “at what point will it no longer be necessary for us to keep the personal data in this document?” Keeping the document is not necessarily the same as keeping the data. Consider:

Is it necessary to keep the information to prove who signed these documents?
Is the reason for keeping the document to prove the transaction and parties to it?
Is there any risk of a breach of contract claim (which could be claimed up to 6 years after the contract ended, or 12 years if it was signed by deed) and would keeping this personal data be useful in defending any such claim? If not, then it is probably not necessary to keep the data for the full 6 or 12 years even if the document in which it is contained needs to be kept for that long.

1. Accounting Records – generally 6 years

E.g. cheques, invoices, payroll information, tax information, debtor accounts.

In most cases the reason for keeping the document is to prove the transaction and parties to it, so it can't easily be anonymised.

Specific rules will apply to certain records, e.g. pension records,

2. Building records – generally 12 years

E.g. Title deeds, leases, architect or builder contracts, planning permissions, health and safety assessments.

Many of these will have been signed by deed, and so will need to be kept for 12 years. Others will be contractual agreements, and should be kept for 6 years or longer depending on how long the risk against which we would want to cover ourselves using the document might last. However, the question will be whether they should be made anonymous, since it is more likely to be the terms and conditions rather than the personal details that will be useful.

3. Complaints records – generally 6 years

E.g. Complaints about clients, employees, schools, contractors, partners, suppliers.

The reason for keeping these documents will usually be to prove what happened and who was involved, so it can't easily be anonymised, but as time goes on there will be less need to include some details. Records about safeguarding issues are the exception and should be kept permanently.

4. Corporate Records – generally permanently

Some documents may be kept for a specific time, e.g. Insurance settlements and employee grievance settlement agreements, which will be kept for 6 or 7 years after the claim to make sure no further repercussions arise from the original problem.

Others will need to be kept permanently. E.g. registers of directors' interests, members' interests, persons with significant control of the company, trustee minute books, meeting

minutes, court orders. Most of these will need to be kept to comply with statutory requirements which will need us to be able to demonstrate who had what interest and who did what in the running of the company. But otherwise, transactions or relevant events will have limitation periods of 6 – 12 years and personal details contained in these documents may no longer be necessary to keep after this time.

5. Health and Safety Records – generally permanently

E.g. RIDDOR reports and accident books, reports about injuries and surrounding relevant documentation.

There will be statutory rules around how long certain documents and details have to be kept, but the personal data within those documents and others of relevance may become less useful after a certain period of time. The trouble with making a judgment is that personal injury claims can be brought at any point that an injury becomes apparent and attributable to an event in the past – so someone may find in 20 years' time that an injury has developed as a result of something done during their time with us. Proving that will of course get harder as time goes on, so the judgment about what to keep "just in case" has to be proportionate to the likelihood of it happening and how useful any particular piece of personal data would be if an issue did arise.

6. Human resources records – generally 6 (or 7) years after employment ends

E.g. staff records, overtime records, redundancy records, life assurance expressions, work documents created by the employee

Some of these will have statutory requirements attached to them, like medical scheme records which need to be held permanently, and others will be a matter of judgment. For example, someone might need to find emails and documents created by the employee which contain their data after seven or eight years following their employment, for a reason other than a claim regarding that person's contract – it could be about piecing together company history for a reason that goes back further. But we can't just keep everything "just in case". The question is whether we need to actually keep the *personal data* within those documents, but if the data cannot be removed from the document, the possibility of someone wanting to find out something from 7 years ago may not be a realistic enough reason to keep hold of the document.

Other records, such as candidate information collected from unsuccessful applicants, will not need to be held for anything like 6 years. It is not likely to actually be useful for any more than 6 months or so.

Schedule 10: Data Security Breach Procedures (Planning a Response to a Data Security Breach)

A data security breach can happen for a number of reasons:

- Loss or theft of data or equipment on which data is stored;
- Inappropriate access controls allowing unauthorised use;
- Equipment failure;
- Human error;
- Unforeseen circumstances such as a fire or flood;
- Hacking attack; and
- ‘Blagging’ offences where information is obtained by deceiving the organisation who holds it.

However the breach occurred, there are five important elements to any breach-management plan. As such, this policy is structured as follows:

1. Containment and recovery – the response to the incident, including production of a recovery plan and, where necessary, procedures for damage limitation.

2. Assessing the risks – assessment of any risks associated with the breach, as these are likely to affect what we do once the breach has been contained. Consider the potential adverse consequences for individuals; how serious or substantial these are; and how likely they are to happen.

3. Notification of breaches – informing people about an information security breach. Consider who needs to be notified and why. This might include the individuals concerned; the Information Commissioner’s Office (ICO); other regulatory bodies; other third parties such as the police and the banks; or the media.

4. Evaluation and response – investigate the causes of the breach and also evaluate the effectiveness of our response to it. If necessary, update our policies and procedures accordingly.

5. Informing the ICO – in some circumstances, the ICO needs to be involved, and so the final part of this policy will focus on this specifically.

Containment and recovery

Data security breaches will require not just an initial response to investigate and contain the situation but also a recovery plan including, where necessary, damage limitation. This will often involve input from specialists across the business such as IT, HR and legal and in some cases contact with external stakeholders and suppliers.

The very first step is that whoever discovers a breach will report it to the Data Protection Lead for their team. They will then report it in turn to the Data Protection Officer who will help to coordinate a response with the Data Protection Lead. The Lead should provide the Officer with:

- what data has been lost (what kind, the volume, whether it can identify the individuals)
- to whom it was sent
- the context of the situation
- any measures taken to limit the risk or prevent the spread of the data

The Data Protection Officer will consider the following:

- Decide on who should take the lead on investigating the breach and ensure they have the appropriate resources.

- Establish who needs to be made aware of the breach and inform them of what they are expected to do to assist in the containment exercise. This could be isolating or closing a compromised section of the network, finding a lost piece of equipment or simply changing the access codes at the front door. How can the problem be contained?
- Establish whether there is anything we can do to recover any losses and limit the damage the breach can cause. As well as the physical recovery of equipment, this could involve the use of back up tapes to restore lost or damaged data or ensuring that staff recognise when someone tries to use stolen data to access accounts.
- Where appropriate, inform the Leadership Team, the Board of Trustees, or other relevant organisations such as the police.

Assessing the risks

Some data security breaches will not lead to risks beyond possible inconvenience to those who need the data to do their job. An example might be where a laptop is irreparably damaged but its files were backed up and can be recovered, albeit at some cost to the business. While these types of incidents can still have significant consequences, the risks are very different from those posed by, for example, the theft of a customer database, the data on which may be used to commit identity fraud. Before deciding on what steps are necessary further to immediate containment, assess the risks which may be associated with the breach. Perhaps most important is an assessment of potential adverse consequences for individuals, how serious or substantial these are and how likely they are to happen.

The following are also likely to be helpful in making this assessment:

- - the nature, sensitivity and volume of the data lost
- - the ease of identification of individuals from the lost data
- - the severity of the consequences for those affected
- - any special characteristics – i.e. children or sensitive data
- - the number of affected individuals.

In addition, the following specific considerations will be considered:

- What type of data is involved?
- How sensitive is it? Remember that some data is sensitive because of its very personal nature (health records) while other data types are sensitive because of what might happen if it is misused (bank account details)
- If data has been lost or stolen, are there any protections in place such as encryption?
- What has happened to the data? If data has been stolen, it could be used for purposes which are harmful to the individuals to whom the data relate; if it has been damaged, this poses a different type and level of risk
- Regardless of what has happened to the data, what could the data tell a third party about the individual? Sensitive data could mean very little to an opportunistic laptop thief while the loss of apparently trivial snippets of information could help a determined fraudster build up a detailed picture of other people
- How many individuals' personal data are affected by the breach? It is not necessarily the case that the bigger risks will accrue from the loss of large amounts of data but is certainly an important determining factor in the overall risk assessment

- Who are the individuals whose data has been breached? Whether they are staff, customers, clients or suppliers, for example, will to some extent determine the level of risk posed by the breach and, therefore, our actions in attempting to mitigate those risks
- What harm can come to those individuals? Are there risks to physical safety or reputation, of financial loss or a combination of these and other aspects of their life?
- Are there wider consequences to consider such as a risk to public health or loss of public confidence in an important service we provide?
- If individuals' bank details have been lost, consider contacting the banks themselves for advice on anything they can do to help us prevent fraudulent use.

Notification of breaches

Where we consider that the loss is likely to result in a risk to the rights and freedoms of an individual, we will notify the ICO without undue delay and in any case within 72 hours from the time we are aware of the breach.

To identify if that risk exists, the DPO will consider:

- the nature, sensitivity and volume of the data lost
- the ease of identification of individuals from the lost data
- the severity of the consequences for those affected
- any special characteristics – i.e. children or sensitive data
- the number of affected individuals.
- current guidance from the ICO regarding evaluation of risk

The notification for the ICO will contain:

- the numbers and categories of individuals concerned (e.g. employees, consultants, pupils)
- the categories and numbers of records concerned (e.g. employment records, attendance records)
- description of likely consequences
- description of measures taken to mitigate or recover, prevent and redress and inform.

Where we consider that the loss is likely to result in a high risk to the rights and freedoms of an individual, the DPO will also communicate with the data subjects without undue delay. We will tell them in clear and intelligible language who is affected, in what way, and what we're doing about it.

If, however, the data is unintelligible or encrypted to the point that it is not useable, or where we manage to completely recover the data, we will not inform the individual. We will however inform the ICO.

Even if we decide that the loss is not likely to result in a risk to the rights and freedoms of an individual, we will log the breach and explain in our log why the decision was made not to disclose it.

If we are a processor rather than a controller, we will notify the controller without undue delay.

Where the DPO determines that there should be a notification of individuals, they must then consider who to notify, what we are going to tell them and how we are going to communicate the

message. This will depend to a large extent on the nature of the breach but the following points may be relevant to our decision:

- Is there a relevant regulatory body? A sector specific regulator may require us to notify them of any type of breach but the ICO should only be notified when the breach involves personal data.
- What is the most appropriate method of notification? Always bear in mind the security of the medium as well as the urgency of the situation.
- Our notification should at the very least include a description of how and when the breach occurred and what data was involved. Include details of what we have already done to respond to the risks posed by the breach.
- When notifying individuals, we need to give specific and clear advice on the steps they can take to protect themselves and also what we are willing to do to help them.
- Is there a way in which they can contact us for further information or to ask us questions about what has occurred – a helpline number or a web page, for example?
- If we are to notify the ICO, we should also include details of the security measures in place such as encryption and, where appropriate, details of the security procedures we had in place at the time the breach occurred. We should also inform them if the media are aware of the breach so that they can manage any increase in enquiries from the public.
- If we are informing the media, it is useful to inform them whether we have contacted the ICO and what action is being taken. ICO will not normally tell the media or other third parties about a breach notified to them, but they may advise us to do so.
- Do we need to consider notifying third parties such as the police, insurers, professional bodies, bank or credit card companies or trade unions?

Evaluation and response

It is important not only to investigate the causes of the breach but also to evaluate the effectiveness of our response to it. Clearly, if the breach was caused, even in part, by systemic and ongoing problems, then simply containing the breach and continuing 'business as usual' is not acceptable; similarly, if our response was hampered by inadequate policies or a lack of a clear allocation of responsibility then it is important to review and update these policies and lines responsibility in the light of experience.

We may find that existing procedures could lead to another breach and we will need to identify where improvements can be made.

The following points will assist us to review our procedures:

- Make sure we know what personal data is held and where and how it is stored. Dealing with a data security breach is much easier if we know which data are involved. Our notification with the Information Commissioner will be a useful starting point.
- Establish where the biggest risks lie. For example, how much sensitive personal data do we hold? Do we store data across the business or is it concentrated in one location?
- Risks will arise when sharing with or disclosing to others. We should make sure not only that the method of transmission is secure but also that we only share or disclose the minimum amount of data necessary. By doing this, even if a breach occurs, the risks are reduced
- Identify weak points in our existing security measures such as the use of portable storage devices or access to public networks

- Monitor staff awareness of security issues and look to fill any gaps through training or tailored advice
- Consider whether we need to establish a group of technical and nontechnical staff who discuss ‘what if’ scenarios – this would highlight risks and weaknesses as well as giving staff at different levels the opportunity to suggest solutions
- Consider implementing a plan for data security breaches similar to our Business Continuity Plan for dealing with serious incidents
- Identify a group of people responsible for reacting to reported breaches of security.

Informing the ICO

Breaches will be notified to the ICO by the DPO using the DPA security breach notification form which should be sent to the email address: casework@ico.gsi.gov.uk, or by post to the office address: Wycliffe House, Water Lane, Wilmslow, Cheshire SK9 5AF.

The security breach notification form can be found here:

http://www.ico.org.uk/for_organisations/data_protection/lose.aspx

The nature and seriousness of the breach and the adequacy of any remedial action taken will be assessed and a course of action determined. The DPO will inform the Chair of Audit Committee immediately of any reportable breach likely to lead to regulatory action.

The ICO may:

1. Record the breach and take no further action, or
2. Investigate the circumstances of the breach and any remedial action, which could lead to:
 - no further action;
 - a requirement on us to undertake a course of action to prevent further breaches;
 - formal enforcement action turning such a requirement into a legal obligation; or
 - where there is evidence of a serious breach of the Data Protection Act 2018 / GDPR, whether deliberate or negligent, a monetary penalty.

Informing the Charity Commission

The Charity Commission may consider a breach to be a serious incident for the purposes of the Serious Incident Reporting requirements.

The Commission has released guidance saying that the following will count as Serious Incidents for these purposes:

1. The Charity’s data has been accessed by an unknown person; this data was accessed and deleted, including the charity’s email account, donor names and addresses;
2. A charity laptop, containing personal details of beneficiaries or staff, has been stolen or gone missing and it’s been reported to the police;
3. The Charity’s funds have been lost due to an online or telephone ‘phishing scam’, where trustees were conned into giving out bank account details;
4. A Data Protection Act breach has occurred and been reported to the ICO.

Therefore, if a report is made to the ICO, a report must be made to the Commission. The DPO will arrange this in consultation with the Corporate Governance team in line with the applicable Serious Incident Reporting procedures (including consultation/notification of Audit & Finance Committee and any other relevant parties).

Schedule 11: Archive Policy Statement and Procedure

Archive Policy Statement

Education Development Trust generally works with clients that require us to keep documents for certain numbers of years, usually six but sometimes 12. We are obligated to keep operational documents, financial documents, sometimes very broadly described “project documents”. The reason is so that we can demonstrate, if challenged, the services we provided and the invoices involved. In addition to this we work under statutory obligations that require us to keep certain documents for certain periods of time. Finally, documents generated under contracts with no specific retention period may be needed for a period of six years following the end of that contract due to the limitation period on contractual claims and disputes.

Some of this documentation will include personal data, which we do not have to keep in order to demonstrate those things our clients need or to comply with statutory obligation. Therefore, it is our intention not to normally archive documents on a project containing personal data. However, sometimes personal data cannot be removed from documents. In some cases, the effort and resource required to identify and remove personal data would be disproportionate to the impact on the data subjects from our keeping it. In these situations, we will balance the rights of and risks to the data subjects against our own legitimate needs to retain documentation and, where we determine that the need to keep it prevails, we will only keep such documentation for as long as we believe it is necessary for us to do so and will take such measures as are reasonable to mitigate any risk to the data subjects concerned.

An Archive Procedure form will be completed when documents are to be archived, and a record will be kept of the form.

Archive Procedure

When a project ends or an employee leaves, documents (which may or may not contain personal data) will need to be either destroyed or stored. To decide which, consider the following questions:

Project name / Business Area:

Client name (if relevant):

Description of documentation:

Archive box number / electronic folder location:

Question 1 – reason for keeping documents

1. Is there a contract governing the project, or under which the documents were generated (including an employment contract)? [Yes / No]
2. Does that contract (or any law or regulatory obligation) require that we store documentation for a set period of time? [___ years]
3. If not, is the documentation required for the purposes of demonstrating what took place during the contract (i.e. services provided, financial transactions, problems encountered, etc)?

[Yes - Keep it for six years after the contract ends]

No - Does any other factor mean it is necessary to keep it and, realistically, how long will it remain necessary to keep it and how frequently should this decision be revisited?

[Reason: _____]

Question 2 – personal data in documents

1. Does the documentation contain personal data or (if it is not reasonably practicable to check) is it reasonable to assume personal data is contained within the documentation?
[Yes / No]
2. If so, what impact will our continuing to hold that personal data have on the individuals and what is your assessment of the risk to those individuals if the information were to be disclosed to others?

[Risk of holding - [minimal]/[acceptable]/[high]

Risk from disclosure - [minimal]/[acceptable]/[high]

Likelihood of disclosure - [minimal]/[acceptable]/[high]

3. If the reason for keeping the documentation identified in Question 1 is anything other than a legal obligation or a contractual obligation, is it reasonable to believe that the likelihood of risk to the individuals and the impact of that risk is outweighed by the need to keep the documentation? [Yes / No]
4. Is it possible to reduce the possible impact on individuals by taking any other action (removal of personal data from the documentation, making any data anonymous, extra security measures etc?) – if so those measures should be implemented prior to archive.

[Reasonable mitigations (if any) – anonymisation / deletion / extra security / other:
_____]

Decision

1. We are obliged to keep the documentation for _____ years; OR
We have a legitimate business need to keep the documentation for _____ years subject to reviewing this decision every _____ months/years]

2. We consider that we are justified in continuing to hold any personal data in the documentation for the period identified above; AND
We consider the risk to individuals to be [minimal]/[acceptable]/[high] and have done what can reasonably be done to minimise risk]

Signed by project manager:

Signed by Data Protection Lead:

[Signed by Data Protection Officer (where Lead considers appropriate):]

Schedule 12: Marketing and Electronic Communications

Introduction

Education Development Trust does need to send out service updates or legitimately needed information from time to time. We will not disguise marketing information amongst these communications. We will provide direct marketing materials to individuals only if they have expressly agreed to receive it, whether it is direct mail, telemarketing, automated calls, emails or SMS.

Education Development Trust will only use opt-in consent (i.e. “tick this box if you would like to receive” vs “by submitting this application form you agree to receive”). This will apply to all forms of communication for these purposes.

If we receive a written notice from any individual requesting that we do not process their data for the purposes of direct marketing (the communication of advertising or marketing material to particular individuals), we will take steps to cease any direct marketing to that person and cease processing their data in that manner.

The Privacy and Electronic Communications Regulations (PECR) says that we must have opt-in consent for sending direct marketing communications. Data Protection Act 2018 / GDPR says we must have a lawful basis (consent, contract, legitimate interests) for using people’s contact details for other kinds of communications.

1. A “marketing” communication is one that:

- advertises, describes, promotes or draws attention to us, a service or an event. Conducting surveys would not count, since that would not promote, advertise, describe or draw attention to us or a service.
- is sent to the public or in a public medium (i.e. not a targeted offer to a targeted individual, and not to a business) – social media counts.
- is intended (at least partly) to increase sales or public awareness (i.e. not for a specific purpose).

2. If something is “marketing” then we need to have the person’s consent to send it to them (or they need to have consented to. Hence, if we want to add someone to a generic mailing list that sends out updates to people in a non-targeted fashion, then we would need to be sure the people on that list had consented.

3. If something is not “marketing” then the normal Data Protection Act 2018 / GDPR principles apply and we do not necessarily need the consent of the individual in two situations:

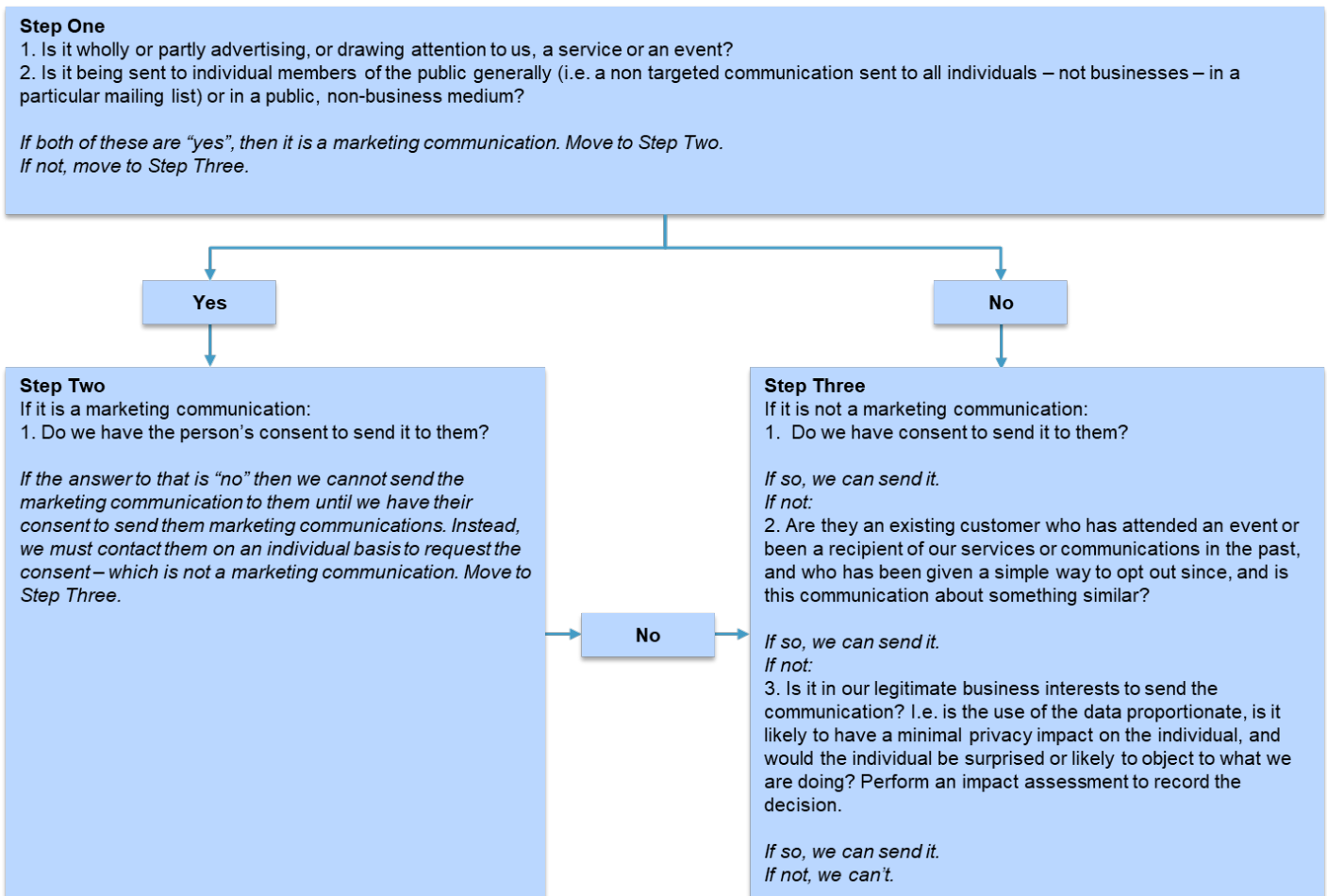
- We can use the basis of our legitimate business interests if the use of the data is proportionate, has a minimal privacy impact, and people would not be surprised or likely to object to what we are doing.
- If they are an existing customer who has attended an event or been a recipient of our services in the past, and we gave them a simple way to opt out both when we first collected their details, we do not need to ask them again for consent.

4. Electronic communications sent to businesses are not covered by the PECR (because they are not communications sent to the public). But if that business uses personal email addresses, Data Protection Act 2018 / GDPR will apply and we need to decide if we can use that personal email address to contact the business without the person's consent (which we probably can, because we have a legitimate business interest in doing so and there will be no negative impact on the individual – quite the opposite in fact – but we would need to fill out a data impact assessment to demonstrate our thinking in that respect).

5. Contact details in the public domain cannot simply be added them to a mailing list which targets the public generally for “marketing”, because the person would not have agreed to receive that information from us. However, contact details on public directories etc can be legitimately used to contact those people provided it is fair and lawful and is not “marketing”.

Electronic communications: Checklist

When planning to send an electronic communication containing information about a service or event, consider the following:



Schedule 13: Data Protection Annual Review Procedure

Data Protection: Annual review of effectiveness procedure

Review and effectiveness

The Data Protection Officer and Data Protection Leads will meet quarterly to discuss data protection in their business areas and flag areas of concern to be addressed.

On an annual basis, the Data Protection Officer will review the data protection environment. This will include reviewing and updating the Data Protection Policy and reviewing completed Self-Assessment Reports from all Data Protection Leads. The review will focus on:

- what has gone well
- problems encountered by the Leads, including data breaches and teething / implementation issues
- the number of data erasure / portability / DSAR / other personal subject access requests received and whether they were dealt with well or if problems were encountered
- suggestions for revisions to the policy
- questions or misunderstandings amongst team members
- common areas of weakness, i.e. have teams fallen back into sharing passwords or failing to encrypt etc

This annual review will ensure that controls are functioning effectively by:

1. Reviewing the activities of those individuals with access to personal data, to ensure that they are handling data in accordance with regulations, and that there is still a business case for them to have those rights in respect of the data they are handling. This will involve looking at each activity to determine if the initial reasoning for collecting, handling and storing the personal data is still valid. Where there is no longer a valid reason, this should be noted as a concern.
2. Reviewing those individuals who have left roles with access to protected personal data, to ensure that access rights have been removed.
3. Reviewing the personal data being held, to ensure that there is still a business case for it to be held or used and to assess whether data that is no longer needed has been deleted or destroyed or returned.

The results of the review should be forwarded to the Data Protection Officer along with any issues or concerns arising. The Data Protection Officer will then undertake an annual review of data protection across the organisation to identify any issues and ensure adequate action is taken.

The results of the annual review will be summarised in a report to the Audit & Finance Committee. Any identified actions from the annual review will be monitored via the quarterly Data Protection Lead meetings.

Related Documents

- Annual Review Self-Assessment Report – Guidance
- Annual Review Self-Assessment Report
- Self-Assessment Report Dashboard template for AFC
- Annual Report to AFC

Schedule 14: Security

Security: Organisational

Education Development Trust will ensure that access to personal data is restricted to those who need access to it in order to perform their legitimate tasks, in line with any consent provided by the individual to whom that data refers or any exemption that applies.

Physical documents containing personal data will not be left in unlocked cupboards or boxes, or in other unsecured areas, on desks overnight or taken home by employees without the knowledge of the Data Protection Lead. Outside organisations such as cleaners or caterers will not be permitted to access areas in which personal data is held or stored without agreeing to appropriate data protection and confidentiality commitments.

Employees will not disclose their passwords to other employees or third parties, or allow other people to access their email accounts or individual folders in which personal data is stored, unless it is necessary for a legitimate work-related reason and only on a restricted or temporary basis wherever possible.

Employees will be aware of the seriousness of emails being accidentally sent to the wrong address. Where an email containing personal data has been sent to the wrong address, and particularly when it has been sent to an external individual, employees must report any such mistake to the Data Protection Lead as soon as it happens.

When personal data is to be destroyed, paper or microfilm records will be disposed of by shredding or incineration.

Security – technical

Education Development Trust will implement appropriate technological safeguards against unauthorised or unlawful processing of personal data and against accidental loss or destruction of data. This may include: encryption of laptops and password protections, firewalls and other measures against cyberattacks, monitoring the security levels of and restricting access to (and the use of) any server/cloud based hosting service if personal data is hosted on it.

Screens of computers should be locked when not attended.

Electronic materials containing personal data will not be stored on employees' personal devices or emailed to unsecured personal email addresses. Employees will not use USB sticks or other portable devices to remove personal data from the Education Development Trust servers.

We will conduct regular testing of the strength of the measures in place, including penetration testing, to identify areas of concern. The Data Protection Lead for the Information Technology department will ensure that Education Development Trust's technical security measures are in place and updated.

When personal data is to be destroyed, computer hard disks, USB storage devices and external or portable hard drives will be destroyed, re-formatted or permanently over-written.

Schedule 15: ICO Registration

Education Development Trust is registered with the ICO as a data controller and will ensure its entry in the register is up-to-date.

The Information Commissioner's Office (ICO) and Data Protection Act 2018 / GDPR requires that Education Development Trust (and each school) holds a record of the data processing activities it undertakes. Education Development Trust has a record registered with the ICO and the form is at Schedule 6 together with an example form for the schools to hold and keep updated.

Data is held by Education Development Trust to enable us to achieve our charitable objectives in the field of education, in accordance with our Articles of Association. In particular we use personal data to provide education and training to our customers and clients; to promote and provide our services, to maintain our own accounts and records and to support and manage our employees. We also use CCTV for security and the prevention and detection of crime.

We hold data for the following specific purposes:

1. Staff Administration (including recruitment and payment)
2. Contracting with clients and partners
3. Organisation and administration of projects and courses
4. Realising the charity's Charitable Objectives
5. Monitoring of health and safety arrangements and records
6. Maintaining accounts & employee records
7. Monitoring of performance and achievements
8. Advertising, Marketing & Public Relations
9. Information and Database Administration
10. Journalism and Media
11. Research
12. Processing outside the European Economic Area ("EEA") where necessary for work being carried out in other countries
13. Compliance with statutory obligations of local authorities, government agencies and other bodies
14. Complying with requests made to client organisations under the Freedom of Information Act or providing information under relevant contracts to client organisations
15. Other relevant purposes, which will be indicated to individual subjects from time to time

Schedule 16: Data Privacy Frequently Asked Questions (FAQs)

Topic Area	Question	Answer
Data Breaches	Who do I contact if I think there may have been a data breach?	Please immediately report this to your Data Protection Lead and the Data Protection Officer.
Data Breaches	When it comes to notifying the ICO of data breaches, does the 72 hours start from the time of the data breach or the time that we become aware of it?	We must report a notifiable breach to the ICO without undue delay, but not later than 72 hours after becoming aware of it. If we take longer than this, we must give reasons for the delay.
Data Breaches	With regards notifying the ICO of data breaches, is the 72 hours based on working days?	<p>The 72 hours starts from when we become aware of a data breach. In all likelihood, we will generally become aware of a breach during the working week and we then have 72 hours to notify the ICO if needed.</p> <p>The 72 hours after becoming aware of a data breach do include public holidays and weekends.</p>
Data Breaches	If we believe that we have received personal data from someone else in error, which we think might be a breach, do we have a duty to report it?	<p>If we were to receive an email plainly intended for someone else and attaching a huge list of personal details, then we could reasonably assume that this was a breach. So, in that situation we would inform the sender that they'd sent it to the wrong place and then delete the data (rather than inform the ICO).</p> <p>We would have had no right to receive it, no legitimate justification for keeping it (with the exception of certain exempt situations such as prevention of crime of national security – if we receive something like that then we wouldn't delete it but report it to the police) and so we would not be able to hold onto it.</p>
Data Subject Rights	What is personal data?	Any information by which a living individual can be identified either on its own or in conjunction with other information you already know e.g. Name, DOB, address, photographs etc. The use of personal data is regulated by the law, which applies to anyone who processes or stores personal data. It also protects the rights of those individuals over their own personal data.
Data Subject Rights	What does portability mean?	It is about people being able to ask to have data we hold on them held on a different kind of device or in a different format, mainly for transfer to someone else.

Topic Area	Question	Answer
Data Subject Rights	What happens if someone wants us to forget all their personal data?	<p>Notify your Data Protection Lead and the Data Protection Officer, as this is a Data Subject Access Request (DSAR).</p> <p>Information that we hold because we have to by law we would have to keep. The individual's rights don't extend to those types of data, but the rest would need to go.</p>
Data Subject Rights	Do Data Subject Access Requests (DSARs) have to be in writing? If not, how do we verify if they are genuine?	<p>DSARs should be made in writing, but the ICO's guidance is that: "you do not need to respond to a request made verbally but, depending on the circumstances, it might be reasonable to do so (as long as you are satisfied about the person's identity), and it is good practice to at least explain to the individual how to make a valid request, rather than ignoring them."</p>
Data Subject Rights	Could you confirm that we don't get the 3-month extension (as we do for DSAR) if the request for deletion, transfer or amendment is excessive?	<p>We can extend the time to respond by a further two months if the request is complex or we have received a number of requests from the individual. We must let the individual know without undue delay and within one month of receiving their request and explain why the extension is necessary.</p> <p>However, it is the ICO's view that it is unlikely to be reasonable to extend the time limit if:</p> <ul style="list-style-type: none"> • it is manifestly unfounded or excessive; • an exemption applies; or • you are requesting proof of identity before considering the request.
Data Subject Rights	How does Data Protection Act 2018 / GDPR affect Education Records?	<p>All current and former pupils, regardless of age, have a right of access to their official educational records held within the Education Development Trust schools and nurseries. While in principle students have a right of access to the whole of their educational records, in exceptional cases some information may be withheld.</p> <p>The main exemptions are for information which might cause harm to the physical or mental health of the student or a third party, information which may identify third parties (for example other pupils) and information which forms part of some court reports. Information may also be withheld if in that particular case it would hinder the prevention and detection of crime or the prosecution or apprehension of offenders to provide it.</p>
Data impact assessments	If there's a new stage coming up on a programme, should we complete a Data Impact Assessment?	<p>Yes, complete a Data Impact Assessment as it is a new, key activity within the programme. It's important to get used to identifying where personal data might be collected/used etc and where it might have an impact on people.</p>

Topic Area	Question	Answer
Data storage	Is it advantageous under the new Data Protection Act 2018 / GDPR rules to be holding all or most of our data within a CRM system to which known people have access and update rights/responsibilities?	Systems that enable data to be identified and located and protected will be helpful, so it might be helpful to restrict access to certain folders to ensure security.
Data storage	A new contact has given me their business card with their details on. Does that mean they can be entered into a CRM system and can I use their email address to send them details about our latest research?	If someone has given you a business card with the intention of having you contact them for a particular purpose, then we should only be using it for that particular purpose and be recording what that purpose is. If we don't have that (which very often we won't – we'll only have it if it's at a seminar where people can sign a collection sheet at the point that they provide us with their contact details) then before adding them to a mailing list we would need their consent. So the first thing to do will be to contact them via those contact details they've given us, to provide them with the data collection information and telling them that we need their opt-in permission to add them to a mailing list. If they opt-in, then we can send them things like our research.
Disclosure of staff information	Are there situations where it is okay to disclose home addresses and telephone numbers of staff/pupils?	Home addresses or telephone numbers of staff or other data subjects must not be given out to third parties unless the individual has given permission to do so. An individual's staff/pupil status is personal data. Education Development Trust should be careful to neither confirm nor deny that the person is a member of staff or a pupil at Education Development Trust school or nursery, or that the person is otherwise known to Education Development Trust.
Email protocol	Is a departmental email address classed as personal data?	A departmental email address e.g. admin@xxx is not classed as personal data as an individual cannot be determined from it. Therefore it is not subject to Data Protection Act 2018 / GDPR. An email address such as headteacher@xxx is classed as personal data as the identity of that individual could be surmised and therefore is subject to Data Protection Act 2018 / GDPR. In order to use that personal email address therefore, we would need to have either consent (which isn't likely), a contract already in place (which is possible), or we are satisfied that we can use our legitimate interests (by performing an impact assessment).
Email protocol	Is it ok to send on emails to internal staff if it contains personal data?	This is fine as it's necessary often to complete their job.

Topic Area	Question	Answer
Email protocol	Is there a difference between sharing personal data between employees of Ed Dev Trust and sharing with external individuals/organisations?	Yes, there is a difference. It is understood that within an organisation, personal data does need to be shared in order for employees to conduct their jobs effectively. However, if personal data is to be shared externally (outside the organisation) then we need to make sure individuals are aware that this is happening to their data. This is covered in the standard data collection form and out privacy notice which are being rolled out across Ed Dev Trust.
Email protocol	Are we no longer able to share people's contact details with another person in our network to reach out to?	In respect of sharing information with other people in the network, that will depend on why the network exists (if it is to carry out a contract, and people are part of it due to contractual commitments, then quite possibly we could justify it that way) and how people came to be in the network (what did they sign, and did they give consent to details being shared across the network) and with whom they are being shared. The principle will always be that people's details should not be shared unless there is a good reason for it and preferably they should have consented to the sharing of their details in that way. As noted in the question above, we are able to share information with colleagues for work purposes, but we need to consider the reasons for why we are passing it on to them e.g. to perform a contract, or whether it is for marketing purposes, and whether the individual (whose details we are sharing) has consented or whether the risk to their privacy is minimal.
Email protocol	Is there standard guidance on what emails should be kept/deleted?	A lot of people will legitimately need their emails from only a few years ago because of audit trails and suchlike, and if it is too difficult or disproportionately costly to go through and anonymise them then we can justify keeping them. Beyond a certain point obviously that justification will not be as strong, so emails kept over 6 years are not going to be useful any longer unless a person is in a particularly important role.
Email protocol	Does data in emails need to be removed as part of a deletion request?	This will need to be determined on a case by case basis. Ideally all data should be deleted i.e. including emails, but we may have a case that the deletion of data (particularly from emails) may be excessive, in which case we can inform the requester of this fact. This will need to be determined at the time and with input from the Data Protection Officer.

Topic Area	Question	Answer
<p>Email protocol</p>	<p>If we already hold e-mails/contact details or they are in the public domain, can we contact the individuals in an unsolicited way to share something or to ask for a targeted response on something rather than a mass mailout?</p>	<p>The point we have to start with is that any kind of marketing communication is only to be sent to people who have agreed to receive it. So, if we happen to obtain a person’s contact details via some method that didn’t include asking them if they wanted to receive anything from us, we shouldn’t be sending that person marketing communications.</p> <p>So, if we already have someone’s contact details, we would need to check with them if they are happy for us to continue to contact them for the purposes of marketing the same way we would with a mailing list. Unless the consent they already gave the first time round was clear, unambiguous and positive (i.e. “I want this” vs “I didn’t say I didn’t want this”) – if it was already then we’d be ok to keep using it under Data Protection Act 2018 / GDPR but the approach we’re taking across the organisation is that we want consent renewed.</p> <p>If someone’s details are in the public domain, genuinely provided in that spirit with the intention that people contact them for certain things, then they can generally be contacted but I would suggest “marketing” communications would not be allowed. So we could send a targeted email asking someone about a project we are doing to invite them to join in, since it isn’t advertising our services generally but a specific and targeted communication about a business opportunity (the like of which they would have intended to receive by putting their details into the public domain for that purpose). But the line will be thin between the two, and if we can possibly obtain consent first we should. And if that isn’t practical, then we should use a Data Impact Assessment to determine whether or not it is appropriate to contact them on the basis that it is a legitimate business interest that will benefit the person and have no negative impact on the use of their data. That will give us a good response if anyone challenged the process.</p> <p>For more guidance on sending emails and what constitutes marketing, see the “Electronic comms” guidance on the intranet page.</p>
<p>Human Resources</p>	<p>How does Data Protection Act 2018 / GDPR affect recruitment and selection?</p>	<p>It is important to ensure that applicants who are responding to job advertisements or completing application forms know exactly to whom or where they are supplying their information and for what their information will be used. Only information relevant to the recruitment decision should be</p>

Topic Area	Question	Answer
		<p>requested. Applicants should have explained to them as early as possible what verification checks may be undertaken.</p> <p>It is important to ensure that personal data used during, and retained after the interview process, is justifiable against any challenge of it being relevant and necessary. Education Development Trust may be asked to prove that the non-selection of a candidate was on the basis of something other than a discriminatory attitude held by the interviewer. Applicants will have subject access rights regarding interview notes taken. It is for this reason that all interview notes must be legible and understandable. It is recommended that interview notes be kept for a period of 6 months after the date of interview.</p>
Human Resources	How does Data Protection Act 2018 / GDPR affect Equal Opportunities monitoring?	<p>The law specifically allows for processing of data on protected characteristics under the Equality Act 2010 if it is necessary for keeping under review the existence, or absence, of equality of opportunity. The collection of this information is exclusively used for the statistical evaluation of the Education Development Trust's equal opportunities policy within recruitment and employment.</p> <p>Education Development Trust, where possible, will ensure anonymity of information when meaningful monitoring is required. The equal opportunities monitoring form, which collects information for this purpose, must be removed from all applications before any assessment of suitability for the post is considered.</p>
Human Resources	How does Data Protection Act 2018 / GDPR affect Discipline, Grievance and Dismissal of employees?	<p>Employees have the same rights of access to files containing information about disciplinary matters or grievances about themselves as they do to other personal data held, unless this information is associated with a criminal investigation, in which case an exemption might apply. All of the normal data protection and access obligations apply to data created or accessed in the course of dealing with disciplinary and grievance issues. Any information referring to a third party must be removed or anonymised before access is granted.</p> <p>Disciplinary warnings typically 'expire' after one year provided that no further warnings have been issued and no disciplinary action has been taken against the employee during that period. In these circumstances, the warnings will generally be disregarded for future disciplinary purposes but</p>

Topic Area	Question	Answer
		<p>not removed from the personal file. There may be occasions, however, for example in the case of gross misconduct, or gross negligence, where the nature of the offence does not make it desirable and practicable for the one year time limit to apply. If this is so, the employee must be notified in writing when the warning is given of the period applicable, which will not normally exceed 5 years. Exceptions to the time limit will apply where child protection issues are raised - refer to the Child Protection procedure for further information.</p> <p>Details regarding information relating to discipline/grievance issues must not be disclosed to a third party. For example, being known as an employee of Education Development Trust may mean being asked, for instance by third parties or parents, about the alleged suspension of another member of staff. Under no circumstances should this information be disclosed or confirmed and persistent enquiries must be referred to the Data Protection Officer.</p>
Human Resources	How does Data Protection Act 2018 / GDPR affect the Disclosure and Barring Service?	<p>Information received via a DBS form will be treated as strictly confidential and only considered in relation to the post being applied for.</p> <p>Once a recruitment (or other relevant) decision has been made, disclosure information should not be kept for any longer than is absolutely necessary. For those applicants who are not appointed this should generally be for a period of up to six months, to allow for the consideration and resolution of any disputes or complaints. Once the retention period has elapsed, Education Development Trust must ensure that any disclosure information is destroyed by secure means.</p> <p>Even for successful applicants neither the application form nor the DBS certificate should be kept. No copies should be held, the certificate should be reviewed and information such as certificate number, issue date and outcome of certificate should be recorded on Business World On! Disclosure information must only be used for the specific purpose for which it was requested and for which the applicant's full consent has been given.</p>
Human Resources	How does Data Protection Act 2018 / GDPR affect Confidential References?	<p>Data subjects (in this context usually employees or former employees) are permitted to access references about themselves received by Education Development Trust (subject to respecting the confidentiality of third parties).</p>

Topic Area	Question	Answer
		<p>Under the Data Protection Act 2018, employees and former employees were not entitled to access references provided by Education Development Trust to third parties in confidence relating to them. It is expected that this exemption will continue to apply under Data Protection Act 2018 / GDPR.</p>
<p>Human Resources</p>	<p>How does Data Protection Act 2018 / GDPR affect Sickness and Accident Records?</p>	<p>Sickness and accident records will include information about an employee's physical or mental health. These types of record should be treated as sensitive personal data and are therefore subject to specific extra requirements under the Act.</p> <p>The Act makes a distinction between sickness, accident and absence records. Sickness and accident records contain details of the illness, condition or accident suffered by the individual. Absence records however, may explain the reason for the absence as 'sickness' or 'accident' but do not include any reference to specific medical conditions. The Information Commissioner recommends that sickness and accident records should be separated from absence records and that sickness and accident records should not be accessed where records of absence could be used instead.</p> <p>In order to hold these records, Education Development Trust has to satisfy at least one of the conditions for processing sensitive personal data. Those conditions that may be most directly relevant to sickness and accident records are:</p> <ul style="list-style-type: none"> • The processing is necessary for the purposes of the exercising or performing any right or obligation, which is conferred or imposed by law on Education Development Trust in connection with employment. This could include obligations under health and safety legislation or for the purpose of administering statutory sick pay. This condition may also be relevant to the need to maintain sickness records so that Education Development Trust can ensure that an employee is not dismissed on sickness grounds, when it would have been unfair to do so. • The processing is necessary for the purpose of, or in connection with, any legal proceedings (including prospective legal proceedings), or is necessary for the purpose of obtaining legal advice, or is otherwise necessary for the purposes of establishing, exercising or defending legal rights. This condition may therefore apply where Education Development

Topic Area	Question	Answer
		<p>Trust is defending itself against tribunal or court proceedings.</p> <ul style="list-style-type: none"> The data subject has given his or her explicit consent to the processing. This will only apply where the employee understands what personal data is involved and has given a positive indication of agreement (such as a signature). The consent must also be freely given and not made subject to a detriment if the employee withholds their consent. <p>Being known as an employee of Education Development Trust may mean being asked for information, for instance by third parties, about another member of staff or a child at a school. Although this can be awkward, third parties should generally be informed that employees are unable to give out personal information to third parties, unless the requester can demonstrate that they have a legitimate reason for requesting the information (like the parents of a child, the police, or a doctor in a medical emergency) in which case their identification will first need to be verified.</p>
Image Capture	How does Data Protection Act 2018 / GDPR affect photographs, videos and CCTV?	<p>Where it is wished to take photographs or make video recordings of staff and/or pupils, as individuals, as small groups or organised groups, the individual(s) concerned must give their consent and be informed of the purpose(s) for which the information is to be used. For general photographs or video recordings of Education Development Trust offices and public places, whereby individuals cannot be identified, consent is not required. If Education Development Trust intends to record an event such as a sports day or school play, the relevant people must be informed of the intention and the purpose(s) for which the recording will be used. The third party may choose to withdraw themselves or their child from such an event if they object to the recording. The standard collection form should be used.</p> <p>Education Development Trust must ensure the recorded images are stored securely, where only a limited number of authorised persons have access to them. The recorded images must only be retained long enough for any incident to come to light (e.g. for a theft to be noticed). Education Development Trust may disclose recordings to a law enforcement agency in order to help with the prevention or detection of crime (see section 8.5) but must not release the images to any other third party. Employees must never take photos, especially of children, on personal devices.</p>

Topic Area	Question	Answer
		It must be remembered that it is not relevant that an individual resides in, or that a photo was taken in, another country even if that country is outside the EEA. The use of the image will be processing of personal data if it takes place within the UK or is hosted on a website to which the UK has access, and so consent of the individual must be sought or an exemption applied.
Obtaining consent	Should we be obtaining opt-in consent for our marketing contacts?	Yes definitely. The contact list needs to be reviewed as with others across the organisation and anyone who does not provide opt-in consent within a reasonable period of time should be removed from the list.
Obtaining consent	If we receive email confirmation of people opting-in to receive our marketing emails, should we retain them?	Yes, any record of consent should be retained as evidence.
Obtaining consent	If we already have proof of opt-in consent, do we need to go back out again to get it again for Data Protection Act 2018 / GDPR?	We do not need to obtain consent again if we have evidence that they have already opted in.
Obtaining consent	Is oral consent valid?	Sometimes yes. It wouldn't be for some things though – like being added to a newsletter mailing list, because we'd find it very hard to prove that they consented if challenged. If we had a realistic way of obtaining consent and recording it then perhaps, but it would be better to avoid it because of the difficulty with proving it.
Obtaining consent	Is it ok to continue to contact people while you are waiting for them to provide a response to the consent opt-in?	To prompt them into responding - yes. There is some disagreement over whether it's ok to email someone for consent to email them, but we have to take a pragmatic attitude to it.
Obtaining consent	How many times can we realistically ask for consent from an individual?	There is no specific guidance on this but realistically a sensible amount of times to follow up would be three times over a period of six months. The onus is on us to try and follow up. Where we can't obtain consent, then we should not be using that individual's personal data.
Obtaining consent	If people's email addresses are public e.g. Ministers, Headteachers, is it ok to contact them to ask them to join events etc?	This is difficult to say for certain. If they are in the public domain for a particular purpose and we want to market to them, then no we shouldn't use them to add to our marketing list. Because what you're effectively doing is adding someone's contact details to your mailing

Topic Area	Question	Answer
		list without having them specifically agree to receive marketing communications from you. If they aren't there for a particular purpose (e.g. their contact details are provided so individuals can contact them), then we should be able to contact them for anything.
Obtaining consent	Would invites to events (e.g. workshops/conferences we are organising) be classed as marketing and therefore require consent?	No – there are no tested definitions of “marketing” but the references throughout the Regulations make it fairly clear that it means non-targeted communication to “the public” (or from a automated mailing list) in order to advertise and promote, rather than a targeted communication for a specific individual for a particular purpose.
Obtaining consent	If we are planning an event, do we need to build a consent option into the invite?	Yes, the invite will need to specify that their details will be added to a database for similar purposes in the future and they will need to consent (e.g. tick box or confirm yes in writing) to this. Alternatively, we could gain that consent in a follow up email following the event, or at the event itself.
Obtaining consent	Could we use social media instead of relying on traditional sign ups to updates on our research?	It is certainly an option, as long as we are not sending anything that counts as “marketing” directly to individuals (unless they have consented to receive research/marketing updates) e.g. tweeting about our latest research report.
Obtaining consent	Could we send new research to individuals via direct messages on LinkedIn?	No – social media is caught by the PECR the same way as any other electronic communication method. If we decide what we want to send is “marketing” then using social media will not get around the requirement for consent.
Obtaining consent	The policy talks about keeping data up to date, should we be going out to contact individuals to confirm their data is still current? If so, how frequently should this be done?	As ever, a pragmatic approach is needed. If you have a date of birth for someone, it isn't likely to need updating. If you have a home address, people might well move every five/ten years or so. If you have an email address, it might change relatively frequently. So it depends on what you're holding, and how likely it is that someone might change it.
Obtaining consent	If a member of staff is being specifically mentioned in a bid e.g. day rates charged (and they often are as we add in CVs to bids to add weight to the quality of the work) is that covered by the employment contract for the member of staff?	The place to start with this is, where did we get the CV? Did the person provide it to us with the intention of our using it in this bid or similar bids? If so, did they specifically consent to it or was it part of a contract we have with them (either way that would give us a legal basis for using the data in this way). There will, most likely, be a genuine basis for our having that information and feeling that we are justified in using it – and the idea would be that we would record the decision to use it in a Data Impact Assessment if it wasn't completely clear,

Topic Area	Question	Answer
		in which we would explain why we considered it appropriate to do so when balanced against the individual's rights.
Obtaining consent	We have a new service/product. We have existing permissions for 'keep me informed with your research'. Can we send info about new services to the same group?	Provided that the consent they have provided was to receive a category of information, and the information about the new service fell within that category, then yes. We would need to just make sure it fell into that category. Which probably means we need to make sure that the consent we collect in the first place is broad enough to cover what we realistically think we'll want to tell people about.
Overseas entities	How does Data Protection Act 2018 / GDPR affect our overseas offices?	Ed Dev Trust's branch offices overseas and outside the EEA will comply with the Data Protection Policy in its entirety, to the extent that they process data regarding EU data subjects and in the context of Ed Dev Trust's activities in the EU. Ed Dev Trust's overseas subsidiary companies that are not branch offices are legally distinct from Ed Dev Trust and are incorporated in overseas jurisdictions such that Data Protection Act 2018 / GDPR will not generally apply to them. Nevertheless, Ed Dev Trust will have in place contracts with all overseas subsidiaries to require those subsidiaries to protect and safeguard data sent to them by Ed Dev Trust in line with the security and privacy requirements of Data Protection Act 2018 / GDPR.
Overseas entities	Although the policy applies to the EU, many/most of the principles can also be applied to our international operations. On that basis, should each overseas entity also appoint a Data Protection Lead?	The overseas processor contract will be put in place with our international entities and branch offices. The manager signing the contract should be responsible for ensuring that overseas entity abides by the terms in the overseas contract. Responsibility for this could be delegated but the role would be different to that of Data Protection Leads.
Overseas entities	Can generic guidance of data protection best practice (do's and don'ts) be shared with international entities?	These are available on the intranet page .
Technology	How does Data Protection Act 2018 / GDPR affect data on the Internet?	Data placed on Education Development Trust's web site and made available via the Internet will be available in countries which do not have a data privacy regime considered adequate by the EU. Where Education Development Trust wishes to make staff/pupils personal data available in this way, the consent of the staff and/or student(s) concerned must be obtained. Consent can be withdrawn at any point. Internet pages are sometimes used to collect personal data such as names and addresses of

Topic Area	Question	Answer
		<p>Individuals who request Education Development Trust information e.g. from those who are registering to attend an event. The relevant web page should indicate the purpose or purposes for which the data is collected, the recipients to whom it may be disclosed and an indication of the time period for which it will be kept (e.g. "while we process your application", rather than a specific date).</p> <p>All web sites that collect information from site visitors must provide a Privacy Statement. The purpose of this statement is to help individuals to decide whether they want to visit the site and, if so, whether to provide any personal information. Privacy Statements must be prominently displayed.</p> <p>Individuals must be given the opportunity to opt out of parts of the collection or use of the data not directly relevant to the specific purpose.</p>
Technology	How does Data Protection Act 2018 / GDPR affect the usage of apps in schools?	<p>Teachers may wish to use educational apps as part of their teaching and learning methodology in schools. As these apps are provided by third party providers, it is necessary that these apps are vetted before they are used in the classroom. The Schools' Data Protection Leads are responsible for monitoring the apps that are being used in their school and ensuring that parental consent is obtained for the use of these apps. Teachers must make their School's Data Protection Lead aware of any new app(s) they would like to use in their classrooms so that the School's Data Protection Lead can review the app provider for compliance with the General Data Protection Regulations.</p>
Working with suppliers	Who is responsible for sending the overseas processor contract to our overseas offices?	Whoever is in charge of the contract should send the overseas processor contract.
Working with suppliers / partners / contractors	How does Data Protection Act 2018 / GDPR affect due diligence when working with suppliers, partners and contractors?	When undertaking new work and working with new partners/suppliers/contractors, the Due Diligence process must be used. This includes the need for the Trust to obtain copies of the partner's/supplier's/contractor's Data Protection policies so that we can ensure that they are compliant with the General Data Protection Regulations.