Data Protection Policy

Board Approved Date	July 2018
Version	0.1
Author Initials	Risk Management Team (ZW)
Review Date	June 2021

(This policy supersedes all previous Data Protection policies)

Amendments

Policy Date	New Version Number	Summary of change	Comments

Contents

NON CONTRACTUAL POLICY

1. Introduction

1.1 Education South West (referred to in this document as 'The Trust') and our schools collects and uses personal information about staff, pupils, parents and other individuals who come into contact with the Trust or individual schools.

1.2 This information is gathered in order to enable it to provide education and other associated functions. In addition, there may be a legal requirement to collect and use information to ensure that the Trust complies with its statutory obligations. The Trust has a duty to be registered, as Data Controllers, with the information Commissioner's Office (ICO) detailing the information held and its use. These details are then available on the ICO's website.

1.3 This policy outlines the framework that governs how The Trust and its staff must handle personal data to ensure compliance with the EU General Data Protection Regulation (GDPR) and associated data protection laws applicable in the UK.

2. Purpose and Statement of Policy

2.1 This policy is intended to ensure that personal information is dealt with correctly and securely and in accordance with the General Data Protection Regulations (GDPR), Data Protection Act 2018, and other related legislation (refer to Appendix 1).

1.1 Specifically under GDPR, this policy applies to the processing of personal data which is defined by article 4 of the GDPR, and to the processing of special categories of personal data defined by article 9 of the GDPR.

2.2 It will apply to information regardless of the way it is collected, used, recorded, stored and destroyed, and irrespective of whether it is held in paper files for electronically.

2.3 The Members, Directors, employees and members of the Local Governing Bodies comply with the requirements and principles of GDPR and the Data Protection Act 2018. All staff involved with the collection, processing and disclosure of personal data are aware of their duties and responsibilities within these guidelines.

2.4 Enquiries for further information about the Data Protection policy is available from the Trust Data Protection Officer.

2.5 General information about GDPR and the Data Protection Act can be obtained from the office of the Information Commissioner (website http://ww.ico.gov.uk).

3. What is Personal Information

3.1 For the purpose of this policy, personal data refers to information that relates to an identifiable, living individual, including information such as

NON CONTRACTUAL POLICY

an online identifier, e.g. an IP address. The GDPR applies to both automated personal data and to manual filing systems, where personal data is accessible according to specific criteria, as well as to chronologically ordered data and pseudonymised data, e.g. key-coded.

3.2 Sensitive personal data is referred to in the GDPR as 'special categories of personal data'. These specifically include the processing of genetic data, biometric data and data concerning health matters.

4. Data Protection Principles

4.1 GDPR and the Data Protection Act 2018 is underpinned by six common-sense principles which governs the way that all schools within the umbrella of ESW must process personal data.

4.2 These principles are outlined in article 5 of the GDPR and are summarised below.

- *Personal data shall be processed lawfully, fairly and in a transparent manner in relation to the data subject ('lawfulness, fairness and transparency').*
- *Personal data shall be collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes.*
- *Personal data shall be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed ('data minimisation')*
- *Personal data shall be accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay ('accuracy')*
- *Personal data shall be kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed.*
- *Personal data shall be processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures ('integrity and confidentiality').*

5. Lawful Processing of Personal Data

5.1 The Trust and its staff must process personal data fairly and will not process personal data or special categories of personal data unless one or more of the following lawful grounds listed is applied

a) The data subject has **given consent** to the processing of his or her personal data for one or more specific purposes.

b) Processing is necessary for the **performance of a contract** to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract.

c) Processing is necessary for **compliance with a legal obligation** to which the controller is subject.

d) Processing is necessary in order to **protect the vital interests** of the data subject or of another natural person.

e) Processing is **necessary for the performance of a task** carried out in the public interest or in the exercise of official authority vested in the controller.

f) Processing is necessary for the purposes of the **legitimate interests** pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child.

6. Privacy Notices

6.1 When collecting personal data, The Trust will make available the information contained in our Privacy Notice 'Pupil and Parent Information: Protection and Use of Information'. This is a statement which explains our policy regarding the personal information we collect.

7. Consent

7.1 The Trust is only required to obtain someone's consent if there is no other legal basis for processing their personal data. If we are required to obtain consent, we will ensure that the following requirements are met;

- The consent is freely given
- The person giving consent understands fully, what they are consenting to
- There must be a positive indication of consent (opt-in as opposed to opt-out)
- The person giving consent must be able to withdraw their consent at any time
- Consent should be documented so that it may be referred to in the future, if necessary

8. Rights of Data Subjects

8.1 Chapter 3 of the GDPR outlines the rights afforded individuals in respect of the processing of their personal data. These rights are summarised below;

- The right to transparency in respect of the processing of their personal data
- The right of subject access
- The right to rectification
- The right to erasure
- The right to restriction of processing
- The right to data portability
- The right to object to processing
- The right to request human intervention if processing is by automated means

8.1 Requests to exercise any of these rights are managed by the ESW Data Protection Office (DPO).

8.2 When designing, implementing or procuring systems or services, The Trust must ensure that those systems or services can allow members of the public to exercise any of the rights listed above. Any systems or services found to be incapable of managing such requests, should be referred to the Data Protection Officer (DPO) and must be subject to a Privacy Impact Assessment.

8.3 Please refer to the Data Subject Rights Procedure.

9. Privacy by Design

9.1 The Trust and its schools will act in accordance with the GDPR by adopting a privacy by design approach and implementing technical and organisational measures which demonstrate how the Trust has considered and integrated data protection into processing activities.

9.2 Data protection impact assessments (DPIAs) will be used to identify the most effective method of complying with the Trust's data protection obligations and meeting individuals' expectations of privacy.

9.3 As per Article 29 of the GDPR, DPIAs will be undertaken on all new systems, processes or procedures that intend to process personal data, prior to their implementation. Such assessments are to be carried out by or in consultation with the Data Protection Officer.

10. Security Incident Management and Notification

10.1 The breach of security which has led to the destruction, loss, alteration, unauthorised disclosure of, or access to, personal data is called a 'personal data breach'.

10.2 Examples of activities considered an information security incident might include; information being at risk of or being lost; stolen; disclosed to the wrong recipients (accidentally or deliberately); accessed or attempted to be accessed unlawfully and/or without the permission of the School; sold or used without the permission of the School or a system containing personal data or sensitive business data malfunctions and the information is irretrievable indefinitely or for a long period of time.

10.3 The Trust's DPO will ensure that all ESW staff members are made aware of, and understand, what constitutes a data breach as part of their CPD training. Staff must report any data breach or potential breach as soon as possible to the Data Protection Officer or the ESW Business Manager.

10.4 In accordance with article 33 of the GDPR, The Trust is committed to notifying the Information Commissioner's Office (ICO) or relevant supervisory authority within 72 hours, of being notified of an information security incident that might adversely affect the rights and freedoms of a data subject. Notifications of this nature are the responsibility of the Data Protection Officer, who will ensure that the risks associated with information security incidents are recorded, monitored and where appropriate escalated.

11. The Data Protection Officer

11.1 Under Article 37 of the GDPR The Trust has appointed a Data Protection Officer to undertake the tasks outlined in article 39 of the GDPR. Contact details for the Data Protection Officer are made publicly available and will be referred to in all privacy notices.

11.2 The Trust has committed to ensure that the Data Protection Officer is sufficiently resourced to undertake the tasks assigned to them under article 39 of the GDPR. The Trust will also ensure that the Data Protection Officer is consulted on all matters which concern the processing of personal data.

11.3 The Data Protection Officer will act as the single point of contact for the Information Commissioner's Office or other relevant supervisory authorities and will ensure that compliance risks are reported to the highest level of management, i.e. The Trust Board as required.

12. Transfers Outside of the European Economic Area

12.1 The Trust will not transfer personal data to countries outside of the European Economic Area (EEA) unless one or more of the following qualifying criteria are met;

1) An adequacy decision has been made in accordance with article 45 of the GDPR

2) The transfer is the subject of appropriate safeguards in accordance with article 46 of GDPR
3) The transfer is the subject of binding corporate rules in accordance with article 47 of the GDPR
4) If one or more of the special circumstances outlined in article 49 of the GDPR are met

13. Information and Cyber-Security

13.1 The Trust undertakes to ensure security of personal data by the following general methods (precise details cannot, or course, be revealed.

13.2 Appropriate building security measures are in place, such as entry key pads, alarms, window bars, deadlocks. Only authorised persons are allowed in the server room which is locked when not in use. Disks, tapes and printouts are locked away securely when not in use. Visitors to the school are required to sign in and out, to wear identification badges whilst in the school and are, where appropriate, accompanied.

13.3 Security software is installed on all computers. Only authorised users are allowed access to the computer files and password changes are regularly undertaken. Computer files are backed up (i.e. security copies are taken) regularly.

13.4 In order to be given authorised access to the computer, staff will have to undergo checks and will sign a confidentiality agreement. All staff are trained in their Data Protection obligations and their knowledge updated as necessary. Computer printouts as well as source documents that have personal, or sensitive personal, data on them are shredded before disposal.

13.5 Overall security policy for data is determined by the Directors of the Trust and is monitored and reviewed regularly by nominated shared services staff, especially if a security loophole or breach becomes apparent. Any queries or concerns about security of data in the Trust should be in the first instance be referred to the Trust Data Protection Officer.

13.6 Individual members of staff can be personally liable in law under the terms of the Data Protection Acts. They may also be subject to claims for damages from persons who believe that they have been harmed as a result of inaccuracy, unauthorised use or disclosure of their data. A deliberate breach of this Data Protection Policy will be treated as a disciplinary matter, and serious breaches could lead to dismissal.

14. Sharing Personal Information

14.1 The Trust and the schools within the Trust will only share personal data contained in its records with individuals who have a legitimate and legal right to view or receive it. Disclosures of personal data shall be proportionate and necessary and made in line with the School's policies and procedures. All disclosures shall comply with the GDPR

and associated data protection legislation, Human Rights Act 1998 and Common Law Duty of Confidence.

15. Information Assurance and Compliance

15.1 The Trust has in place an assurance framework to aid in the implementation and ongoing compliance with the new Data Protection legislation.

15.2 The DPO will ensure that monitoring of the Trust's compliance with the GDPR, Data Protection Act 2018 and other laws, including managing internal data protection activities, advising on data protection impact assessments, conducting internal audits, and providing the required training to staff members takes place.

16. Review of policy

16.1 This policy is reviewed every three years by the Trust in consultation with the recognised trade unions. We will monitor the application and outcomes of this policy annually to ensure it is working effectively.

APPENDIX 1

Legislation

ESW processes a variety of personal data to enable us to deliver a range of education services. Therefore, ESW is required to comply with the GDPR as well as other supporting legislation which governs the processing of personal data.

When handling and managing information ESW, its schools and its staff shall comply with other legislation in addition to the GDPR, to include but not limited to:

- Computer Misuse Act 1990
- Copyright Designs and Patents Act 1988
- Environmental Information Regulations 2004
- Equality Act 2010
- Freedom of Information Act 2000
- Human Rights Act 1998
- Local Government Act 1972
- Local Government Act 2000
- Regulation of Investigatory Powers Act 2016
- Re-use of Public Sector Information Regulations 2005

APPENDIX 1

Definitions

"Personal data"	means any information relating to an identified or identifiable living individual
"Identifiable living individual"	identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data or an online identifier, or one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of the individual.
"Processing"	means obtaining, recording, organising, structuring or storage, adaptation or alteration, retrieval, consultation or use, disclosure by transmission, dissemination or otherwise making available, alignment or combination or restriction, erasure or destruction.
"Data Subject"	means the identified or identifiable living individual to whom personal data relates.
"Parent"	has the meaning given in the Education Act 1996, and includes any person having parental responsibility or care of a child.
"Filing system"	means any structured set of personal data which is accessible according to specific criteria, whether held by automated means or manually and whether centralised, decentralised or dispersed on a functional or geographical basis.
"Pseudonymisation"	means the processing of personal data in such a manner that the personal data an no longer be attributed to a specific data subject
"Controller"	means the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data
"Processor"	means a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller

"Third party"	means a natural or legal person, public authority, agency or body other than the data subject, controller, processor and persons who, under direct authority of the controller or processor, are authorised to process personal data
"Consent"	of the data subject means any freely given, specific, informed and unambiguous indication of the data subject's wishes