Data Protection Policy

0161 Education CIC

Policy Owner	0161 Education CIC
Reviewed Date	29/10/24
Next Review Date	29/10/25
Reviewed By	Jozef Chlebik

0161 Education helps children and young people shift their mindset to make positive choices for themselves and those around them. We care about the individual. We commit to each programme. We provide change.

1. Introduction

The UK General Data Protection Regulation (UK GDPR) is a UK law which came into effect on 01 January 2021 and sets out the key principles, rights and obligations for most processing of personal data in the UK, except for law enforcement and intelligence agencies.

It is based on the EU GDPR (General Data Protection Regulation (EU) 2016/679) which applied in the UK before that date, with some changes to make it work more effectively in a UK context, The DPA 2018 sets out the framework for data protection law in the UK.

It was amended on 01 January 2021 by regulations under the European Union (Withdrawal) Act 2018, to reflect the UK's status outside the EU. It sits alongside and supplements the UK GDPR - for example by providing exemptions. It also sets out separate data protection rules for law

enforcement authorities, extends data protection to some other areas such as national security and defence, and sets out the Information Commissioner's functions and powers.

0161 Education is committed to protecting the privacy of individuals and handles all personal information in a manner that complies with the UK GDPR. The organisation has established the following policy to support this commitment. It is the personal responsibility of all employees (temporary or permanent), Governors, contractors, agents, volunteers and anyone else processing information on our behalf to comply with this policy.

Any deliberate breach of this policy could amount to a criminal offence under one or more pieces of legislation, for example the Computer Misuse Act 1990, the UK GDPR or the Data Protection Bill. All incidents will be investigated and action may be taken under the organisation's formal disciplinary procedure. A serious breach of this policy could be regarded as gross misconduct and may lead to dismissal and / or criminal action being taken.

This policy explains what our expectations are when processing personal information. This policy should be read together with the Information Security Policy, Information Security Acceptable Use Policy, Protective Marking Scheme, and the Organisation Records Retention and Disposal Schedule.

2. The Data Protection Principles and Definitions

The UK GDPR is concerned with the use (processing) of personal data.

Personal data is information that either on its own, or when combined with other information, can be used to identify a living individual. Examples of personal data include: - names, addresses, dates of birth, photographs, IP Addresses, Vehicle Registration Plates, CCTV footage. The UK GDPR also defines personal information that is more sensitive and must be treated with a higher level of privacy and respect. This is called Special Category Data.

Special Category Data is any data that falls into the following categories: - racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, genetic data, biometric data such as fingerprints, sexual history or sexual orientation, any data relating to physical or mental health conditions.

Processing Data is referred to throughout the UK GDPR and data protection legislation. This means any use of the personal information. This includes collecting, disclosing, destroying, archiving and organising.

Data Subject is the person who the personal data is about. For example, the children named on a class register at a organisation are all data subjects of that register.

Data Controller is usually an organisation who dictates the reason and purpose for how data is processed. The Organisation itself is a Data Controller as it chooses how it collects, uses and shares its own data.

The Information Commissioner's Office (ICO) is the regulator for Data Protection and Privacy law in the UK. They have the power to enforce on organisations for breaches of the Data Protection Act or the UK GDPR. This means they can issue:

- An Undertaking which commits an organisation to improving their Data Protection practices.
- An Enforcement Notice ordering that an organisation does something specific e.g. train all staff to a high standard.
- A Monetary Penalty for serious and significant breaches. Under the Data Protection Act, this can be anything up to £500,000. Under the General Data Protection Regulation this can be up to £17.5 million or 4% of a company's global turnover.

The Principles

The UK GDPR contains a number of Principles that must be met in order to use personal date in line with the law.

Personal Date must be;

Processed fairly, lawfully and transparently
Processed for a specified and legitimate purpose
Adequate, relevant and limited to what is relevant
Accurate and up to date
Kept no longer than necessary
Stored securely using technical and organisational measures

Principle One - Fair, Lawful and Transparent

Fair and Transparent

When the organisation collects personal information from an individual, we must inform them of what we intend to do with that information once we have it. This is called a Privacy Notice.

The Privacy Notice must include the following information:

- Who will own the data (normally the organisation)
- What the information will be used for.
- The legal basis for collecting and using the information.
- Who the information will be shared with.
- How long the information must be kept for and how it will be stored.
- What Rights under the UK GDPR that the data subject has.
- How they can complain.
- How they can complain to the Information Commissioner's Office.
- Whether the data is stored outside of the UK.
- Whether any automated decisions are made using the information The Privacy Notice must be given to the data subject as soon as possible when collecting their information and this can be done online, through the post or in the form of a recorded voice message. As long as the Privacy Notice is provided, it can take any form necessary.

Lawful

To use information lawfully, the organisation must ensure that no laws are broken when processing the data. This means we cannot use data to break any other laws within the UK.

The organisation will ensure that its processing of personal data fulfils the appropriate general condition(s) for processing outlined in the UK GDPR and Data Protection Act 2018.

The organisation can use personal information if it meets one of the condition in Article 6 of the UK GDPR:

- The data subject has consented to their information being used. This consent must be specific, informed and freely given. The data subject must know what they are consenting to and be given a genuine choice, before consent can be classed as appropriately obtained.
- The personal data is being used to perform a contract with the data subject or to undertake actions necessary for creating a contract with the data subject.
- The personal data has to be processed because legislation says that the Organisation has to. This also applies when the organisation receives a court order that demands disclosure of information.
- The personal data is used in line with the vital interests of the data subject. This is usual a life or death situation.
- The personal data is used in line with a public function or legal power that the organisation is meeting. For example, the Children's Act 1989 gives the organisation the power to look after children at risk of harm. This power also allows the organisation to use information to complete this function.

If the organisation wishes to use Special Category (Sensitive) Data as categorised above, they must meet a lawful basis under Article 6 of the UK GDPR and a separate condition for processing under Article 9. These do not have to be linked.

There are 10 conditions for processing special category data in Article 9 of the UK GDPR. Five of these require additional conditions and safeguards set out in UK law, in Schedule 1 of the DPA 2018.

a) Explicit Consent The Organisation has obtained explicit consent from the data subject. This means that they have been explicitly told everything that will happen with their sensitive data once it has been given to the Organisation.
b) Employment, social security and social protection (if authorised by law)The processing is necessary for the Organisation's obligations of employment law or social security.
c) Vital interests The use of information is in the vital interests of the data subject. As above, this is a life or death situation.
d) Not-for-profit bodies The use of information is necessary for the legitimate aims of a political party, religious group or similar not for profit organisation such as a trade union.
e) Made public by the data subject The personal information has been made public deliberately by the data subject.
f) Legal claims or judicial acts The use of the information is necessary for pursuing or defending a legal claim or whenever the courts need to use data.

g) Reasons of substantial public interest (with a basis in law) The use of data is necessary and in the public interest when a public authority is acting using a legal power written into law. This is the same as the public function condition in the list above. It is also known as a "legal gateway".
h) Health or social care (with a basis in law)The use of the data is necessary for the purposes of preventative or occupational medicine, this also includes the provision of social care.
i) Public health (with a basis in law)The use of the data is necessary for public health purposes such as the prevention of serious diseases or handling cross-border health issues such as pandemics.
j) Archiving, research and statistics (with a basis in law)The use of information is for archiving purposes such as historical archiving or scientific research in the public interest.

When relying on conditions (b), (h), (i) or (j), the Organisation will meet the associated condition in UK law, set out in Part 1 of Schedule 1 of the DPA 2018.

- Employment, social security and social protection
- Health or social care purpose
- Public Health
- Research

When relying on the substantial public interest condition in Article 9(2) (g), the organisation will meet one of 23 specific substantial public interest conditions set out in Part 2 of Schedule 1 of the DPA 2018:

The 23 substantial public interest conditions are set out in paragraphs 6 to 28 of Schedule 1 of the DPA 2018:

- Statutory and government purposes
- Administration of justice and parliamentary purposes
- Equality of opportunity or treatment
- Racial and ethnic diversity at senior levels
- Preventing or detecting unlawful acts
- Protecting the public
- Regulatory requirements
- Journalism, academia, art and literature
- Preventing fraud
- Suspicion of terrorist financing or money laundering
- Support for individuals with a particular disability or medical condition
- Counselling
- Safeguarding of children and individuals at risk
- Safeguarding of economic well-being of certain individuals
- Insurance
- Occupational pensions
- Political parties
- Elected representatives responding to requests
- Disclosure to elected representatives
- Informing elected representatives about prisoners
- Publication of legal judgments

- Anti-doping in sport
- Standards of behaviour in sport

Principle 2 - Specified and Legitimate Purpose

The organisation must only use, collect and share information for a specified and legitimate purpose. This purpose must be in line with the organization's aims and values and not contradict any laws or moral obligations.

Once we have collected information for a specific purpose, we must only use that information for purposes compatible with the original aim.

For example, if the organisation collects information for student care purpose, we can use it for other student care purposes such as evaluating the quality of the service provided. However, we couldn't use student information to inform on non-academic outcomes as this is not a compatible purpose because it so different to the original purpose for collecting the information

Principle 3 - Adequate, Relevant and limited to what is necessary

The organisation must only use, collect or share the information that we need in order to complete the purpose we are trying to achieve. For example, if the organisation only needs to collect a name and address in order to complete the purpose, only then only the name and address should be collected.

Principle 4 - Accurate and up to date

The organisation must ensure that all of its information is as accurate as possible. This means that if we find out something new about a data subject such as a change of address, organisation systems are updated as soon as possible to reflect this change. Inaccurate information can lead to breaches, such as letters or emails being sent to wrong recipients or the wrong decisions being made about people on the back of inaccurate information.

Principle 5 - Kept no longer than necessary

The organisation has a responsibility to ensure that information is retained for the correct amount of time, and no longer. All of the organisations information has a date by which is should be securely deleted or archived. This is written into the organisation's Retention Schedule.

Principle 6 - Stored securely

The organisation must take all appropriate technical and organisational measures to keep information secure and prevent it from being lost or put at risk of being seen by people who shouldn't have access to it. This can take a variety of forms. Examples of technical and organisational measures can be found below.

- Technical Measures
- Firewalls
- Anti-virus software

- Encryption
- Secure emails such as Egress
- VPNs (Virtual Private Networks)
- Transport Layered Security Organisational Measures
- Policies and Procedures in place to help staff understand their duties under data protection
- Training
- User guides for staff
- A more knowledgeable and open culture towards data protection

3. Access and use of personal information

Access and use of personal information held by the organisation is only permitted to employees (temporary and permanent), Governors, contractors, agents, volunteers and anyone delegated access as part of their official duties.

Organisation's information is held on a need to know basis, meaning that unauthorised or inappropriate use of the information is strictly forbidden. Organisation employees must only access information that they have a professional and legitimate need to see. Just because an employee has access to a specific system does not mean that the employee has the right to access all records within that system. Employees must only access cases or files that are directly relevant.

Any deliberate or malicious access to systems or records will be dealt with in line with the Organisation's Disciplinary Procedures. There are also a range of criminal offences under the Computer Misuse Act 1990 and in Data Protection law for unauthorised use, obtaining or destruction of personal data. These offences can be punished by up to 12 months in prison or a fine of up to £1,000.

All organisation employees are responsible for ensuring they process personal data as outlined in organisation policies, procedures and guidance and are required to keep all information secure and confidential.

4. Disclosing personal information

Personal information must only be shared when the staff member receiving the information is satisfied as to the legal basis for sharing the information. 0161 Education staff must ask appropriate questions to ensure the requester (whether internal staff or an external partner) has the appropriate legal reason to see the information they are requesting.

Where necessary, staff members are encouraged to speak to their line manager to ask advice, or contact the Data Protection Officer.

If personal information is given to another organisation or person outside of the organisation, the disclosing person must identify their lawful basis for the disclosure (see section 4 above) and record their decision for sharing, along with the written request for information.

This should include;

- A description of the information given
- The name of the person and organisation the information was given to
- The date
- The reason for the information being given
- The lawful basis.

If an Information Sharing Agreement (ISA) exists, this should be adhered to.

In response to any lawful request, only the minimum amount of personal information should be given. The person giving the information should make sure that the information is adequate for the purpose, relevant and not excessive.

When personal information is given internally or externally, it must be shared using a secure method.

5. Accuracy and Relevance

It is the responsibility of the staff who receive personal information to make sure so far as possible, that it is accurate and up to date. Personal information should be checked at regular intervals, to make sure that it is still accurate. If the information is found to be inaccurate, steps must be taken to correct it. Individuals who input or update information must also make sure that it is adequate, relevant, clear and professionally worded.

6. Retention and disposal of information

The organisation holds a large amount of information. The UK GDPR requires that we do not keep personal information for any longer than is necessary. Personal information should be checked at regular intervals and deleted or destroyed when it is no longer needed, provided there is no legal or other reason for holding it.

The organisation's Records Retention and Disposal Schedule must be checked before records are disposed of, to make sure that the retention period for the information in question, has been served.

For specific information regarding retention and disposal of personal data, consult the organisation's head of centre.

7. Rights of the data subject

Individuals have a number of Rights under the UK GDPR and they are able to enact them against any organisation at time they choose. The Rights include:

- The Right of Subject Access – the right to request a copy of data held about them by an organisation and find out how it is used.

- The Right of Rectification – the right to ask for inaccurate or incorrect information to be corrected or removed.

- The Right of Data Portability – the right to move data from one organisation to another. This could apply when a student moves to another alternative provision.

- The Right to Be Forgotten (Erasure) – the right to ask for data to be removed by the organisation that holds it.

- The Right of Restriction – the right to stop information being used whilst a complaint is made.

- The Right of Objection – the right to ask an organisation to stop using their data. This is particularly used with regards to direct marketing.

The organisation has 30 days (one month) to respond to an individual's request to enact their Rights. This is provided the applicant has put their request in writing and suitable identification has been supplied.

Further information about the rights of the individual can be found in the organisation's Information Rights Policy.

8. Transfer outside of UK

Any transfer of personal data outside the Uk must comply with the UK GDPR and Data Protection Act 2018. The Data Protection Officer must be consulted prior to any transfer of personal data outside of the UK.

9. Reporting security incidents

As a Data Controller (organisation that owns data), the organisation has a responsibility to monitor and investigate all incidents that occur within the organisation that involve any of the principles being breached.

All incidents need to be identified immediately, reported using the Data Breach form. All incidents will be investigated by the Data Protection Officer.

Where an incident occurs, staff must inform the Data Protection Officer as soon as possible. The organisation has a responsibility to report all serious incidents to the Information Commissioner's Office within 72 hours of discovery. All correspondence with the ICO must be approved by the Headteacher/Data Protection Officer.

Staff are advised to contain all incidents of data loss as quickly as possible, either by retrieving information sent in error, locking down erroneous access or asking accidental recipients of organisational data to confirm it has been deleted.

All relevant incidents and risks that are identified should be reported to the Data Protection Officer, regardless of how trivial they may seem. The organisation must constantly evaluate and improve its data protection and information security practices to address the new risks it uncovers. This is to stop breaches from occurring or reoccurring as the case may be.

Specific procedures have been developed for the reporting of all information security incidents and weaknesses. It is designed to make sure that all relevant information is communicated correctly so that timely corrective action can be taken.

All employees (permanent, temporary and external users) must be aware of the procedures and obligations in place for reporting the different types of incidents and weaknesses which may have an impact on the security of the organisation's information assets.

10. Data protection by design

The organisation will meet the requirements of the UK GDPR by building data protection into all new projects from the start and employing appropriate technical and organisational measures to keep personal data secure. This will be achieved through completing Data Protection Impact Assessments (DPIAs).

All new projects must be subject to a DPIA before they can be put out to tender. This step is mandatory and must not be ignored.

A DPIA is a process of assessing the risks to privacy and to personal data in a project. A DPIA enables the organisation to identify risks and problems at an early stage in the project, meaning that changes can be made quickly and without incurring expenses.

11. Responsibilities

Chair of Governor and Governing Body

Overall strategic responsibility for ensuring the organisation complies with relevant legislation.

Head of Centre

To guide the organisation's priorities and policy decisions, including ensuring all organisation functions comply with relevant legislation. To make decisions with regards to the organisation's compliance with the UK GDPR.

Data Protection Officer

To oversee the organisation's compliance efforts with the UK GDPR. To train and provide advice to staff with regards to data protection. To monitor, audit and document all data protection measures taken within the organisation.

All Staff

To adhere to all policies procedures and guidance and to ensure they understand their own responsibilities when handling personal data.

Contact and Data Protection Officer (DPO)

0161 Education CIC has appointed a DPO in order to:

- Inform and advise 0161 Education and its employees about their obligations to comply with the UK GDPR and other data protection laws.

- Monitor 0161 Education's compliance with the UK GDPR 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. The DPO will operate independently, their role being to:

- Advise the organisation and its employees about the obligations to comply with UK GDPR and other data protection requirements – this could be to assist in implementing a new CCTV system or to respond to questions or complaints about information rights.

- Monitor your organisation's compliance with UK GDPR, advising on internal data protection activities such as training for staff, the need for data protection impact assessments and conducting internal audits.

- Act as the first point of contact with the Information Commissioner's Office and for individuals whose data you process.

- Where advice and guidance offered by the DPO is rejected by the organisation, this will be independently recorded.

- Advice offered by the DPO will only be declined at the direction of the Head and/or Governing body and will be provided to the DPO in writing.

- The Organisation centre manager is available for advice and guidance regarding all aspects of data protection and UK GDPR.