Data Protection and GDPR Policy and Procedure

2022-2023

NEWREFLEXIONS
Where every child matters

This policy includes the following sections:

- GDPR Data Protection Policy
- Data Breach reporting
- Subject access request recording

General Data Protection Regulations

Introduction

The General Data Protection Regulations (GDPR) defines UK law on the processing of data on identifiable living people. It is the main piece of legislation that governs the protection of personal data in the UK. Personal information is information about a living individual, who can be identified from the information.

Reflexion Care Group Limited; including the trading names including but not limited to New Reflexions and New Reflexions Education are committed to protecting the privacy of individuals and handle all personal information in a manner that complies with the GDPR. It is the **personal responsibility** of all employees (temporary or permanent), members, contractors, agents 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 and the GDPR. All breaches will be investigated and appropriate action taken.

This policy explains what the Company's expectations are when processing personal information.

GDPR Principles

The GDPR is supported by a set of 6 principles which must be adhered to whenever personal information is processed. Processing includes obtaining, recording, using, holding, disclosing and deleting personal information.

The GDPR principles state that personal information must:

Be processed fairly, lawfully and transparently	Obtained for a specified, explicit and legitimate purpose	Be adequate, relevant and limited to what is necessary
Be accurate and where necessary up to date	Not be kept longer than is necessary	Be handled ensuring appropriate security

Access and Use of Personal Information

Access and use of personal information held by the Company, is only permitted by employees (temporary or permanent), members, contractors, agents and anyone else processing information on our behalf, for the purpose of carrying out their official duties. Use or access for any other purpose is not allowed. Deliberate unauthorised use and access to copying, destruction or alteration of or interference with any personal information is strictly forbidden.

Collecting Personal Data

When personal information is collected, the 'data subject' (that is the person who the information is about) must be told. This is known as a Privacy Notice. Our Privacy Notice can be found on the school website.

The school does not collect any biometric data e.g. personal information about an individual's physical or behavioural characteristics that can be used to identify that person, such as fingerprints, facial shape, retina and iris patterns, or hand measurements. The school does use CCTV for security purposes, please see further information in this policy.

Personal information collected, must be adequate, relevant and not excessive for the purpose of the collection. A person's name and other identifying information should not be collected where anonymous information would suffice.

If the information is collected for one purpose, it cannot then be used for a different and unconnected purpose without the data subject's consent unless there is another lawful basis for using the information (see below). It must be made clear to the 'data subject' all the purposes that their information may be used for at the time the information is collected.

Lawful Basis for Processing

When we process personal information, we will have a lawful basis for doing so. GDPR provides a list of 'conditions' when we can process personal or 'special category' personal information. This is contained within Article 6 and Article 9 of the Regulations.

The GDPR defines special category personal information as information relating to:

- race and ethnic origin
- political opinion
- religious or philosophical beliefs
- trade union membership
- processing of genetic/biometric data to uniquely identifying a person
- physical or mental health or medical condition;
- sexual life

Whenever we process personal information, it must be able to satisfy at least one of the conditions in Article 6 of the GDPR and when we process 'special category' personal information; it must be able to satisfy at least one of the conditions in Article 9 of the GDPR as well.

We can process personal information if it has the data subject's consent (this needs to be 'explicit' when we process sensitive personal information). In order for consent to be valid it must be 'fully informed' which means the person giving consent must understand what they are consenting to and what the consequences are if they give or refuse consent. Consent must not be obtained through coercion or under duress and should be recorded.

Sharing personal data/information sharing

We will not normally share personal data with anyone else, but may do so where:

- There is an issue with a student or parent/carer that puts the safety of our staff at risk
- We need to liaise with other agencies – we will seek consent as necessary before doing this
- Our suppliers or contractors need data to enable us to provide services to our staff and pupils – for example, IT companies. When doing this, we will:
    - Only appoint suppliers or contractors which can provide sufficient guarantees that they comply with data protection law

- Establish a data sharing agreement with the supplier or contractor, either in the contract or as a standalone agreement, to ensure the fair and lawful processing of any personal data we share
- Only share data that the supplier or contractor needs to carry out their service, and information necessary to keep them safe while working with us

We will also share personal data with law enforcement and government bodies where we are legally required to do so, including for:

- The prevention or detection of crime and/or fraud
- The apprehension or prosecution of offenders
- The assessment or collection of tax owed to HMRC
- In connection with legal proceedings
- Where the disclosure is required to satisfy our safeguarding obligations
- Research and statistical purposes, as long as personal data is sufficiently anonymised or consent has been provided

We may also share personal data with emergency services and local authorities to help them to respond to an emergency situation that affects any of our students or staff.

Subject access requests and other rights of individuals

Subject access requests

Individuals have a right to make a 'subject access request' to gain access to personal information that the school holds about them. This includes:

- Confirmation that their personal data is being processed
- Access to a copy of the data
- The purposes of the data processing
- The categories of personal data concerned
- Who the data has been, or will be, shared with
- How long the data will be stored for, or if this isn't possible, the criteria used to determine this period
- The source of the data, if not the individual
- Whether any automated decision-making is being applied to their data, and what the significance and consequences of this might be for the individual

Subject access requests must be submitted in writing, either by letter or email to the HR Manager. They should include:

- Name of individual

- Correspondence address
- Contact number and email address
- Details of the information requested

If staff receive a subject access request they must immediately forward it to the Head teacher who will contact the HR department.

Alternatively, the subject access request can be forwarded directly to the HR manager

HRadmin@newreflexions.co.uk

New Reflexions

Cruckton

Shrewsbury

Shropshire

SY5 8PR

01939 210040

Children and subject access requests

Personal data about a child belongs to that child, and not the child's parents or carers. For a parent or carer to make a subject access request with respect to their child, the child must either be unable to understand their rights and the implications of a subject access request, or have given their consent.

Children below the age of 12 are generally not regarded to be mature enough to understand their rights and the implications of a subject access request. Therefore, most subject access requests from parents or carers of children at our primary school may be granted without the express permission of the child. This is not a rule and a child's ability to understand their rights will always be judged on a case-by-case basis.

Young people aged 12 and above are generally regarded to be mature enough to understand their rights and the implications of a subject access request. Where information is to be shared due to genuine safeguarding concerns, required by the care home, police, or placing authority the permission of the child will be considered but not always required.

Responding to subject access requests

When responding to requests, we:

- May ask the individual to provide two forms of identification
- May contact the individual via phone to confirm the request was made
- Will respond without delay and within one month of receipt of the request
- Will provide the information free of charge
- May tell the individual we will comply within three months of receipt of the request, where a request is complex or numerous. We will inform the individual of this within one month, and explain why the extension is necessary

We will not disclose information if it:

- Might cause serious harm to the physical or mental health of the student or another individual
- Would reveal that the child is at risk of abuse, where the disclosure of that information would not be in the child's best interests
- Is contained in adoption or parental order records
- Is given to a court in proceedings concerning the child

If the request is unfounded or excessive, we may refuse to act on it, or charge a reasonable fee which takes into account administrative costs.

A request will be deemed to be unfounded or excessive if it is repetitive, or asks for further copies of the same information.

When we refuse a request, we will tell the individual why, and tell them they have the right to complain to the ICO.

Other data protection rights of the individual

In addition to the right to make a subject access request (see above), and to receive information when we are collecting their data, about how we use and process it (see section 7), individuals also have the right to:

- Withdraw their consent to processing at any time
- Ask us to rectify, erase or restrict processing of their personal data, or object to the processing of it (in certain circumstances)
- Prevent use of their personal data for direct marketing
- Challenge processing which has been justified on the basis of public interest
- Request a copy of agreements under which their personal data is transferred outside of the European Economic Area
- Object to decisions based solely on automated decision making or profiling (decisions taken with no human involvement, that might negatively affect them)
- Prevent processing that is likely to cause damage or distress
- Be notified of a data breach in certain circumstances
- Make a complaint to the ICO
- Ask for their personal data to be transferred to a third party in a structured, commonly used and machine-readable format (in certain circumstances)

Individuals should submit any request to exercise these rights to the Head teacher in the first instance. If staff receive such a request, they must immediately forward it to the Head teacher in the first instance where a record of the request will be made.

Requests will be processed in accordance with procedure and utilising the HR manager and DPO support services employed.

The Fitzroy Academy commissions DPO services from Telford and Wrekin Council to include:

- Informing/advising on obligations to comply with GDPR

- Complete annual GDPR data audit
- Completion and sign off of Data Protection Impact Assessments
- Support liaison with the Information Commissioners Office
- Support on data breach investigation
- Annual refresher training
- General GDPR support and advice

We will follow the procedure set out in **appendix 2**

Photographs and videos

As part of our activities, we may take photographs and record images of individuals within our school.

We will obtain written consent from parents/carers, or students aged 18 and over, for photographs and videos to be taken of students for communication, marketing and promotional materials.

Where we need parental consent, we will clearly explain how the photograph and/or video will be used to both the parent/carer and student. Where we don't need parental consent, we will clearly explain to the student how the photograph and/or video will be used.

Uses may include:

- Within school on notice boards or posters and in school magazines, brochures, newsletters, etc.
- Outside of school by external agencies such as the school photographer, newspapers, campaigns
- Online on our school website or social media pages

Consent can be refused or withdrawn at any time. If consent is withdrawn, we will delete the photograph or video and not distribute it further.

When using photographs and videos externally to the company, we will not accompany them with any other personal information about the child, to ensure they cannot be identified.

Use of CCTV

We use CCTV externally of the school site to ensure school security. We will adhere to the ICO's code of practice for the use of CCTV.

We do not need to ask individuals' permission to use CCTV, but we make it clear where individuals are being recorded. Security cameras are clearly visible and accompanied by prominent signs explaining that CCTV is in use.

Any enquiries about the CCTV system should be directed to the Head teacher.

Data protection by design and default

We will put measures in place to show that we have integrated data protection into all of our data processing activities, including:

- Appointing a suitably qualified DPO advisory and support service,
- Only processing personal data that is necessary for each specific purpose of processing, and always in line with the data protection principles set out in relevant data protection law (see section 6)
- Completing privacy impact assessments where the school's processing of personal data presents a high risk to rights and freedoms of individuals, and **when introducing new technologies** (the DPO will advise on this process)
- Integrating data protection into internal documents including this policy, any related policies and privacy notices
- Regularly training members of staff on data protection law, this policy, any related policies and any other data protection matters; we will also keep a record of attendance
- Regularly conducting reviews and audits to test our privacy measures and make sure we are compliant
- Maintaining records of our processing activities, including:
    - For the benefit of data subjects, making available the name and contact details of our HR manager and Explanation of our DPO services and all information we are required to share about how we use and process their personal data (via our privacy notices)
    - For all personal data that we hold, maintaining an internal record of the type of data, data subject, how and why we are using the data, any third-party recipients, how and why we are storing the data, retention periods and how we are keeping the data secure

Data security and storage of records

We will protect personal data and keep it safe from unauthorised or unlawful access, alteration, processing or disclosure, and against accidental or unlawful loss, destruction or damage.

In particular:

- Paper-based records and portable electronic devices, such as laptops and hard drives that contain personal data are kept secure when not in use
- Papers containing confidential personal data must not be left on office and classroom desks, on staffroom tables, pinned to notice/display boards, or left anywhere else where there is general access
- Where paper based personal information needs to be taken off site, staff must sign it in and out from the school office and there must be sufficient security.
- Passwords that are at least 8 characters long containing letters and numbers are used to access school computers, laptops and other electronic devices. Staff and pupils are reminded to change their passwords at regular intervals
- The company is rolling out a programme to ensure that Encryption software is used to protect all portable devices such as USB devices

- Where we need to share personal data with a third party, we carry out due diligence and take reasonable steps to ensure it is stored securely and adequately protected

Disposal of records

Personal data that is no longer needed will be disposed of securely. Personal data that has become inaccurate or out of date will also be disposed of securely, where we cannot or do not need to rectify or update it.

For example, we will shred or incinerate paper-based records, and overwrite or delete electronic files. We may also use a third party to safely dispose of records on the school's behalf. If we do so, we will require the third party to provide sufficient guarantees that it complies with data protection law.

Generally complete school records will be maintained until the student reaches 25 years of age. Please refer to our data retention information for more detail.

Personal data breaches

We will make all reasonable endeavours to ensure that there are no personal data breaches.

In the unlikely event of a suspected data breach, we will follow the procedure set out in appendix 1.

Such breaches in a school context may include, but are not limited to:

- A non-anonymised dataset being published on the school website which shows the exam results of individual students
- Safeguarding information being made available to an unauthorised person
- The theft of a school laptop containing non-encrypted personal data about students

Training

All school staff are provided with data protection training as part of their induction process.

Data protection will also form part of continuing professional development, where changes to legislation, guidance or the school's processes make it necessary.

Monitoring arrangements

The Head teacher is ultimately responsible for reviewing this policy; liaising with New Reflexions HR manager and commissioned DPO support services. This policy will be reviewed as required; at least annually and shared with the Directors.

Appendix 1 – Data Breaches

What to do in the event of a possible data breach/incident

1. Introduction

1.1 This procedure details the necessary steps to take if you have concerns that there has been a breach of personal identifiable information (PII) by New Reflexions employees, members or third parties contracted to provide services.

1.2 Some typical examples of a data breach include, but are not limited to:-

- **Personal Data –** e.g. name; address; telephone number; date of birth; NI number; bank account details
- **Sensitive/Special Personal Data –** e.g. information specifically relating to physical or mental health or condition; race or ethnicity; political opinions; religious beliefs, or beliefs of a similar nature; membership of a trade union or non-membership; sexual life; commission or alleged commission of an offence;

2. What is a possible data breach?

2.1 A breach is where identifiable personal information has been or has the potential to be:

- Viewed or copied by an individual unauthorised to do so,
- Communicated to an unauthorised individual/organisation, e.g. sent to wrong address and opened/read
- Lost or stolen

There are many examples of what constitutes a possible data breach, typical examples are detailed below:

- Loss of mobile phone/laptop or other ICT equipment
- Personal information being emailed/posted/faxed to an unintended recipient or address and read by the individual.
- Loss of information/records relating to individuals and read by an unauthorised person, e.g. a lost file containing personal grant information
- Not keeping information secure; i.e. leaving correspondence on your desk at the end of the working day

2.2 There may be security incidents where Personal data has been given to an unauthorised person (due to a human or procedural error) but the recipient has

not opened/read the data. The data has then been returned or it has been confirmed that it has been destroyed. Cases such as these should be notified to the Head Teacher who will be expected to undertake their own investigation into the security incident and implement actions that will minimise the possibility of a similar incident in the future.

3. What should I do if I become aware of a possible data breach?

3.1 Outside a normal working day

3.1.1 If you become aware of a possible data breach you should report it immediately where you can. If this occurs outside normal working hours, e.g. bank holidays, weekends, etc., please contact your line manager within 24 hours of the incident occurring.

3.2 Normal working day

3.2.1 If a breach occurs or you suspect one has occurred you will need to inform your line manager (who will inform the relevant people; including but not limited to the HR manager and DPO service). The matter must be forwarded within 24 hours of the incident occurring for recording and investigation.

3.2.2 If the incident involves theft or a crime then your line manager (Head teacher) should contact the police and report this. Please make sure you obtain and record a crime reference number from the police where applicable.

3.2.3 If the incident involves the loss or theft of ICT equipment then this should also be logged with the IT manager.

3.2.4 When the matter is reported the following information as a minimum should be to hand:

- Crime reference number given to you by the police (if applicable)
- Police station and constabulary the incident was reported to (if applicable)
- Place, time and date(s) the incident occurred
- Employee and/or team(s) details or 3rd party suppliers involved
- A summary of the information that has been lost, stolen or incorrectly communicated
- A list of the individuals affected or that could be at risk
- A list of organisations that may need to be contacted (e.g. shared service information), if applicable
- Confirmation as to who else in the authority has been informed

3.2.5 When the incident is reported to the Head teacher they will:

- Assess the level of the risk associated with the incident
- Agree the immediate mitigating actions that should take place and who should undertake them including who else needs to be informed (internally and externally)
- Agree who will undertake an investigation into the incident –
- Compare the incident against notification rationale outlined by the Information Commissioners Office (ICO) and notify (after approval by the Directors) if applicable
- Produce or agree the production of a report
- Agree remedial action to be taken
- Communicate any lessons learnt corporately where appropriate

DATA BREACH REPORTING FORM

	Report prepared by: Date	
1	Summary of the event And circumstances	
2	Type and amount of personal data	
3	Actions taken by recipient when they inadvertently received the information	
4	Actions taken to retrieve information and respond to the breach	
	Breach investigated by: Date:	
5	Procedures / instructions in place to minimise risks to security of data	
6	Breach of procedure / policy by staff member	
7	Details of notification to affected data subject Has a complaint been received from Data subject?	
8	Details of Data Protection training provided	
9	Procedure changes to reduce risks of future data loss	

Appendix 2 Subject Access Request Guidance

Please read before filling in the Subject Access Request Form

Which sections should I complete?

Sections 1, 2, 3, and 4 should be completed for all applications.

Sections 5, 6 and 7 (Representative Details and Authority to Release Information to a Representative) should only be completed if the application is being made by a representative (i.e. someone other than the data subject themselves).

What information will help with the processing of my subject access request?

If you cannot provide us with satisfactory proof of identity, your application will be rejected

What information does Reflexion Care Group Limited hold?

Reflexion Care Group Limited only holds information relevant to enable it to conduct its business and to meet its legal obligations, which will include, but is not restricted to, personal information about employees, contractors, customers and young people. Please note that some data may have been reviewed and destroyed where appropriate in accordance with our information retention policies.

Reflexion Care Group Limited is the 'data controller' for certain information held on behalf of certain third parties who contract to Reflexion Care Group Limited who provide certain

How long will it take to get my data?

Once we are satisfied that you meet the criteria for disclosure of data under the Data Protection Act, and have provided sufficient information, you should receive a response within 30 days from the date that we accept your application for processing.

Records may be held in several different locations in paper and electronic formats. If you only require specific information and you clearly state what that is – for example a specific document or IT-only data – then you are likely to get a quicker disclosure.

The form includes a section for giving details if you need a disclosure by a certain date. No guarantee can be given that a disclosure will be completed by that date but we will endeavour to comply with reasonable requests for expedited action.

General Notes

1. We will not acknowledge your application in writing but we will provide you with a reference number when we write to you.
2. When we process information requests for children aged 16 or over and spouses, we require their signature of authority before disclosing data. A separate application form should be completed for each individual and additional fee submitted. Sections, 3 and 4 should be completed by a parent/guardian for a child under 16.
3. The documents that you receive may have data redacted (blacked-out) or contain rough notes that may lack clarity. This is because we aim to supply copies of the original records whenever possible. However, certain records may also include third party information which we cannot release to you under the Data Protection Act, e.g. another person's data, this is removed.
4. We will not disclose information by fax or telephone. Disclosure by post is usually made by first class post to the address you provide in section 2 or, if appropriate, to your representative named in section 5.

Checklist

- ❑ Have you completed all relevant sections of the form?
- ❑ If you are a representative, has your client signed the authority in Section 7 or provided a separate signed note of authority?
- ❑ If you are submitting the form yourself, have you signed the form at Section 4?
- ❑ If you are signing as a parent or guardian of a child under 16, have you provided a photocopy of their full birth certificate, photocopies of any court orders and proof of your parental responsibility?
- ❑ If you are a Representative have you enclosed two pieces of identification from the lists in Section 6
(one from each of A and B)?
- ❑ Have you signed the declaration in Section 4?
- ❑ Have you provided as much information as possible to enable us to find the data you require?

Please send your completed form and any proof of identity required to:

HR manager

Reflexion Care Group Limited

Cruckton

Shrewsbury

SY5 8PR

Tel: 01939 210040

Email:
HRadmin@newreflexions.co.uk

Section 1 – Applicant Details

Title (please tick one):	☐ Mrs ☐ Miss ☐ Ms ☐ Title (please state):
Forename(s):	
Family Name:	
Previous Family Name:	
Other name(s) known by:	
Date of Birth (dd/mm/yyyy):	……../……./……. Male ☐ or Female ☐
Nationality:	
Place of Birth:	
Identifying Information	yroll Number……

Section 2 – Applicant Details

Current Address:	
Postcode	
Daytime Telephone No:	
Email Address:	
Previous Address:	
Postcode:	

Section 3 – Details of Information Required

Please use this space to give us any details about the information you are requesting, for example by stating specific documents you require (use extra sheets if necessary):

Section 4 – Declaration

The information which I have supplied in this application is correct, and I am the person to whom it relates or a representative acting on his/her behalf. I understand that Reflexion Care Group Ltd may need to obtain further information from me/my representative in order to comply with this request.

Signature of Applicant:	Date:

Section 5 – Representative Details

(If completed HM Passport Office will reply to the address you provide in this section)

Name of Representative:	
Company Name:	
Address & Postcode:	
Daytime Telephone No:	
Email Address:	

Section 6 – Proof of the Representative's identity

Please provide copies of two pieces of identification, one from list A and one from list B below and indicate which ones you are supplying.

Please DO NOT send an original passport, driving licence or identity card

List A (photocopy of one from below)		**List B (plus one <u>original</u> from below)**	
Passport/Travel Document	☐	A letter sent to you by the Passport Office	☐
Photo driving licence	☐	Utility bill showing current home address	☐
Foreign National Identity Card	☐	Bank statement or Building Society Book	☐
	☐		☐
	☐		☐

Section 7 – Authority to release information to a Representative

A representative needs to obtain authority from the applicant before personal data can be released. The representative should obtain the applicant's signature below, or provide a separate note of authority.

This must be an original signature, not a photocopy (tip: using blue ink often helps verification).

If the applicant is signing as the guardian of a child under 13, proof of legal guardianship must also be provided.

I hereby give my authority for the representative named in Section 5 of this form to make a Subject Access Request on my behalf under the Data Protection Act 1998.	
Signature of Applicant:	Date:
Signature of Representative:	Date:

Section 8 – Timescale

If you have specific reasons for requiring data by a specific date please give details below:

Date required:
Reason (please state and supply supporting evidence):

Reviewed	*May 2021*
Reviewed	*May 2022*
Reviewed	*August 2022*
Next Review Due	*May 2024*
Reviewed by	*Head Teacher*