The General Data Protection Regulations Policy, Practice and Procedure.

R.E.A.L Education Ltd, R.E.A.L Independent Schools, R.E.A.L Alternative Provision School.

Written: September 2018

Reviewed: September 2020

Reviewed and amended September 2022, including inserts relating to UK Data Protection and Digital Information Bill (UK GDPR, 143 EN 2022-23).

Contents

Policy

Introduction to the General Data Protection Regulations

Policy statement

The Lawful Basis for Processing

The R.E.A.L Data Ecosystem

Individual Rights

Data Controller, Processor and Third Party Supplier

Procedure

Data Sharing

Data Deletion, Disposal & Retention

Data Access

Data Security

Data Readiness

Data Subject Access Procedures

Practice

The Data Protection Officer

Privacy by Design & Privacy Impact Assessments

Data Breaches

Policy

Introduction to the General Data Protection Regulations

Information represents people, therefore it is essential that information is collected and processed legally and with consideration for the people who are represented by the data.

This policy covers the processing of data across the organisation, including the R.E.A.L. Independent School, Alternative Provision School, R.E.A.L Foundation Trust, vocational group provision and other activities delivered by R.E.A.L. LTD, (hereby known collectively as R.E.A.L).

We use the term data processing to cover the collection, ordering, storing, retention, transport and disposal of individual information which can identify living people.

We acknowledge that R.E.A.L is required to collect personal data and sensitive personal data. This information is required in order to care for and educate the young people who attend R.E.A.L provision.

All staff involved with the collection, processing and disclosure of personal data will be aware of their duties and responsibilities by adhering to these guidelines.

Policy statement

The details contained within this policy outline the procedure and practice in R.E.A.L to comply with the General Data Protection Regulations.

This policy outlines what types of data R.E.A.L collect and process.
It also explains how we take care of data and what we do with the data once they leave R.E.A.L. Education.

The policy provides an overview of data collection and processing and is not intended as a hand-book or training manual to outline how each piece of data is collected and processed.

R.E.A.L. Education has a legal obligation to collect and process data in accordance with the General Data Protection Regulations (GDPR).

This policy adheres to all requirements under GDPR and Data protection Legislation

The Lawful Basis for Processing

At R.E.A.L we work with all types of learners and they are identified under two distinctive categories:

1. On roll learners - those young people who are registered as a pupil at either R.E.A.L Independent School or R.E.A.L Alternative Provision School

2. Off roll learners - those young people with R.E.A.L Education who are registered at another school, Local Authority (receiving education other than at school) or part of the R.E.A.L Befriending Service

The lawful basis for processing data relates to the different categories of learner as outlined above.

- We collect and use on roll learner data under the legal obligation category in Article 6 of the General Data Protection Regulation (GDPR); and according to the Education Act 1996 (2011).
- We collect and use off roll learner data under the public task category in Article 6 of the General Data Protection Regulation (GDPR); and according to the Education Act 1996 (2011).
- We process all learner special category data under the above Article 6 statements; and according to the Children's Act 1989 (2004)
- Data Protection and Digital Information Bill 2022.

The lawful basis for processing workforce data is separate to the lawful basis for processing learner data

- We process this information under the contractual obligation in article 6 (1)(b) of the General Data Protection Regulations (GDPR).
  We also process special category data under article 9 (2)(b) of the GDPR.

The R.E.A.L Data Ecosystem

Individual Rights

The GDPR provides eight key principles in ensuring the rights for individuals, and their personal data.

1. The right to be informed

The information you provide to people must be concise, transparent, intelligible, easily accessible, and it must use clear and plain language.

Individuals have the right to be informed about the collection and use of their personal data. This is a key transparency requirement under the GDPR.

You must provide individuals with information including: your purposes for processing their personal data, your retention periods for that personal data, and who it will be shared with. We call this ‘privacy information’.

You must provide privacy information to individuals at the time you collect their personal data from them.

2. The right of access

Individuals have the right to access their personal data and supplementary information.

The right of access allows individuals to be aware of and verify the lawfulness of the processing.

3. The right to rectification

The GDPR includes a right for individuals to have inaccurate personal data rectified, or completed if it is incomplete.

An individual can make a request for rectification verbally or in writing.

You have one calendar month to respond to a request.

In certain circumstances data controllers can refuse a request for rectification.

This right is closely linked to the controller’s obligations under the accuracy principle of the GDPR (Article (5)(1)(d)).

4. The right to erasure

The GDPR introduces a right for individuals to have personal data erased.

The right to erasure is also known as ‘the right to be forgotten’.

Individuals can make a request for erasure verbally or in writing.

Data Controllers have one calendar month to respond to a request.

The right is not absolute and only applies in certain circumstances.

This right is not the only way in which the GDPR places an obligation to consider whether to delete personal data.

5. The right to restrict processing

Individuals have the right to request the restriction or suppression of their personal data.

This is not an absolute right and only applies in certain circumstances.

When processing is restricted, we are permitted to store the personal data, but not use it.

An individual can make a request for restriction verbally or in writing.

We will respond to a request within one calendar month.

This right has close links to the right to rectification (Article 16) and the right to object (Article 21).

6. The right to data portability

The right to data portability allows individuals to obtain and reuse their personal data for their own purposes across different services.

It allows them to move, copy or transfer personal data easily from one IT environment to another in a safe and secure way, without hindrance to usability.

Some organisations in the UK already offer data portability through the midata and similar initiatives which allow individuals to view, access and use their personal consumption and transaction data in a way that is portable and safe.

It enables consumers to take advantage of applications and services which can use this data to find them a better deal, or help them understand their spending habits.

7. **The right to object**

Processing based on legitimate interests or the performance of a task in the public interest/exercise of official authority (including profiling);

Direct marketing (including profiling); and

Processing for purposes of scientific/historical research and statistics.

8. **Rights in relation to automated decision making and profiling.**

The GDPR applies to all automated individual decision-making and profiling.

Article 22 of the GDPR has additional rules to protect individuals if you are carrying out solely automated decision-making that has legal or similarly significant effects on them.

Data Controller, Data Processor & Third Party Suppliers

At R.E.A.L Education, R.E.A.L Independent School, and R.E.A.L Alternative Provision School all areas of the organisation may at some time be classified as a data controller, a data processor or a third party supplier. These intercompany transactions can be complex, and are outlined in the organisational service level agreements.

1. The GDPR applies to 'controllers' and 'processors'.
2. A controller determines the purposes and means of processing personal data. The Directors of R.E.A.L Education, are deemed the 'controllers' and are responsible for this policy.
3. A processor is responsible for processing personal data on behalf of the controller. The headteachers within the Independent School and the Alternative Provision School are deemed the 'processors' in terms of this policy.
4. The centralised services within R.E.A.L Education (HR, and financial services) are also deemed as the data processors on behalf of the Independent Schools.
5. Educational services provided through R.E.A.L Education is undertaken under the definition of a 'third party supplier'.
6. As a processor, the GDPR places specific legal obligations on you; for example, you are required to maintain records of personal data and processing activities. You will have legal liability if you are responsible for a breach.
7. GDPR places obligations on controllers to ensure that contracts with processors comply with the GDPR.
8. The GDPR applies to processing carried out by organisations operating within the EU. It also applies to organisations outside the EU that offer goods or services to

individuals in the EU.

9. The GDPR does not apply to certain activities including processing covered by the Law Enforcement Directive, processing for national security purposes and processing carried out by individuals purely for personal/household activities.

Personal Data

The GDPR applies to 'personal data', meaning any information relating to an identifiable person who can be directly or indirectly identified in particular by reference to an identifier.

This definition provides for a wide range of personal identifiers to constitute personal data, including name, identification number, location data or online identifier, reflecting changes in technology and the way organisations collect information about people.

The GDPR applies to both automated personal data and manual filing systems where personal data are accessible according to specific criteria. This could include chronologically ordered sets of manual records containing personal data.

Personal data that has been pseudonymised – eg key-coded – can fall within the scope of the GDPR depending on how difficult it is to attribute the pseudonym to a particular individual.

The types of learner information that we collect, hold and share include:

- Personal information e.g name, address, date of birth, medical details
- Characteristics e.g. ethnicity, free school meal eligibility, looked after status, individual risk status and special educational needs information (special category data)
- Attendance information e.g sessions attended, absences and absence reasons
- Assessment information e.g attainment levels, learner behaviour and welfare

Why we collect and use this information

We use learner data to:

- Support learning
- Monitor and report learner progress

- Provide appropriate support and care to the learner and their families
- Assess the quality of our services
- Comply with the law regarding data sharing
- Promote the safeguarding and welfare of staff, learners and their families

Sensitive personal data

The GDPR refers to sensitive personal data as “special categories of personal data” (see Article 9).
The special categories specifically include genetic data, and biometric data where processed to uniquely identify an individual.
Personal data relating to criminal convictions and offences are not included, but similar extra safeguards apply to its processing (see Article 10).

Procedure

Data Sharing

We will only share personal information either internally, or with parties outside of R.E.A.L when it is legally appropriate or where we are legally enforced to do so. A privacy notice is available via our website, this is a clear statement outlining how information is shared, with whom, and why.

Collecting and storing learner information

Whilst the majority of pupil information you provide to us is mandatory, some of it is provided to us on a voluntary basis. In order to comply with the General Data Protection Regulation, we will inform you whether you are required to provide certain pupil information to us or if you have a choice in this. We store all learner data in accordance to our GDPR policy.

Who we share learner information with

We routinely share learner information with:

- The relevant local authority (including specialist departments)
- Department for Education
- Commissioning body for the learner
- Transport providers
- Awarding bodies
- Any educational setting supporting the learners programme
- Any educational setting after the learner leaves our care

Why we share pupil information

We do not share information about our pupils with anyone without consent unless the law and our policies allow us to do so.
We share pupils' data with the Department for Education (DfE) on a statutory basis. This data sharing underpins school funding and educational attainment policy and monitoring.
We are required to share information about our pupils with the (DfE) under regulation 5 of The Education (Information About Individual Pupils) (England) Regulations 2013

Data Deletion and Retention.

This section of our policy outlines the specific requirements of different data and can be found in Appendix 1.

In summary:

1. Records for on roll learners are kept in accordance with the data retention and deletion details outlined in Appendix 1:7.
2. Records for off roll learners are only kept on electronic file until the end of Placement or Term in which the learner left the services of R.E.A.L. (Appendix 1:7)
   All records are transferred to the nominated school or Local Authority on request at the end of the placement and deleted from ATMOS server.
   All safeguarding files are transferred at the end of placement.
3. Records Befriending Service off roll learners are kept on electronic file until the end of the financial year in which the learner left the services of R.E.A.L.

Data Subject Access Procedures.

This section of our policy outlines the procedures for responding to data subject access requests made under GDPR.

1. All data held will be subject to the Data Deletion and Retention Policy specified in appendix 1 of this document. This will be reviewed on an annual basis but may be amended within this time frame in response to either internal policy changes (Outlined in section 4 of Data breach Management Plan) or external I.O.C guidance.

2.Requests for information can be made in writing; which includes email, and be addressed to the Data Protection Officer. If the initial request does not clearly identify the information required, then further enquiries may be made.

3. The identity of the requestor must be established using 'reasonable means' before the disclosure of any information is made.

4. Any individual has the right of access to information held about them. Under GDPR all young people aged 13 and above own their data. However this is dependent upon their cognitive ability to understand. The DPO should discuss the request with the child and take their views into account when making a decision.

5. Information will be made free of charge, unless the request is deemed excessive. Where requests are manifestly unfounded or excessive, in particular because they are repetitive, R.E.A.L will:

- charge a reasonable fee taking into account the administrative costs of providing the information; or
- refuse to respond.

Where a refusal to respond has been made, we will explain why to the individual, informing them of their right to complain to the supervisory authority and to a judicial remedy without undue delay and at the latest within one month

6. The response time for subject access requests, once officially received, is within one calendar month. R.E.A.L will extend the period of compliance by a further two months where requests are complex or numerous. If this is the case, we will inform the individual within one calendar month of the receipt of the request and explain why the extension is necessary.

7. The information provided should be done so in a format which is easily accessible to the individual. For example if a request is made via an electronic format then the response may be via the same medium.

8. If there are concerns over the disclosure of information then additional advice will be sought.

Practice

The Data Protection Officer

The GDPR introduces a duty for you to appoint a data protection officer (DPO) or (amended 2022) a Data Compliance Officer, if you are a public authority, or if you carry out certain types of processing activities.

At R.E.A.L the identified Data Protection Officer (DPO) role is defined as:

- Providing assistance to R.E.A.L data controllers, and processors, to monitor internal compliance, inform and advise on data protection obligations,
- Provide advice regarding Data Protection Impact Assessments (DPIAs) and Privacy by Design processes and act as a contact point for data subjects and the supervisory authority.

- Impartial and independent, providing expertise in data protection, adequately resourced, and reporting to the Directors of R.E.A.L Education and the Governors of the Independent Schools.
- An existing employee with additional responsibilities and a member of the internal safeguarding forum.
- DPOs can help you demonstrate compliance and are part of the enhanced focus on accountability.
- Are responsible for the delivery of the policy, procedure and practice contained within this document.

Privacy Impact Assessments

A data protection impact assessment (DPIA) is a process R.E.A.L will use to help identify and minimise the data protection risks of new projects.

Following on from the Data Protection and Digital Information Bill 2022/23 proposed amendments, and the removal of the statutory requirements for DPIA's, as a policy where significant changes are identified to data processes we will continue where appropriate to use the DPIA format to identify both negative or positive impact.

A DPIA is used for certain listed types of processing, or any other processing that is likely to result in a high risk to individuals' interests. R.E.A.L will use the ICO screening checklist as an assessment tool to decide when to do a DPIA.

It is also good practice to do a DPIA for any major project which requires the processing of personal data.

The DPIA will:

1. describe the nature, scope, context and purposes of the processing;
2. assess necessity, proportionality and compliance measures;
3. identify and assess risks to individuals; and
4. identify any additional measures to mitigate those risks.

To assess the level of risk, R.E.A.L will consider both the likelihood and the severity of any impact on individuals. High risk could result from either a high probability of some harm, or a lower possibility of serious harm.

If a high risk is identified and R.E.A.L are unable to identify any controls to mitigate that risk, the DPO will consult the ICO before starting any processing.

The ICO will give written advice within eight weeks, or 14 weeks in complex cases. In

appropriate cases the ICO may issue a formal warning not to process the data, or ban the processing altogether.

Privacy by Design

Privacy by design is an approach to projects that promotes privacy and data protection compliance from the start.

Under the GDPR, R.E.A.L have an obligation to implement technical and organisational measures to demonstrate consideration and integrated data protection into all processing activities. A privacy by design approach will be used when:

- building any new ICT systems for storing or accessing personal data;
- developing legislation, policy or strategies that have privacy implications;
- embarking on a data sharing initiative; or
- using data for new purposes.

Data Breaches

The GDPR introduces a duty on all organisations to report certain types of personal data breach to the relevant supervisory authority. At R.E.A.L this will be reported within 72 hours of becoming aware of the breach.

If the breach is likely to result in a high risk of adversely affecting individuals' rights and freedoms, the DPO will inform those individuals without undue delay.

R.E.A.L, through the role of the DPO have robust breach detection processes, investigation and internal reporting procedures in place. These processes help facilitate decision-making about whether or not to notify the relevant supervisory authority and the affected individuals.

The DPO will ensure a record is kept of any personal data breaches, regardless of any relevant notification or requirements to notify.

There are four important elements to the R.E.A.L data breach management plan:

1. Containment and recovery – the response to the incident should include a recovery plan and, where necessary, procedures for damage limitation. The relevant data controller must be informed and depending on the nature of the data - the ICT Team will be informed through www.realservicedesk.co.uk. An initial decision should be made as to relevant notification to ICO.

2. Assessing the risks – The ICT Strategy group and DPO will assess any risks associated with the breach, as these are likely to affect the actions taken once the breach has been contained. In particular, an assessment will be made regarding 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 can be an important part of managing the incident, but it is not an end in itself. The DPO will decide who needs to be notified and why. For example, consider notifying the individuals concerned; the ICO; other regulatory bodies; other third parties such as the police and the banks; or the media.

4. Evaluation and response – The DPO will investigate the causes of the breach and also evaluate the effectiveness of the response to it. If necessary, the DPO will initiate a full review and update of policies, procedures and practice to the GDPR document.

Appendix 1

Data Deletion and Retention Policy.

Contents

1. Retention Statement
2. Complaints
3. Estates and Facilities
4. Human Resources
5. Information Systems & Information Communications Technology
6. Policies & Procedures
7. Student Records

1. Retention Statement

Records are kept to:

- Meet current and future business needs;
- Comply with G.D.P.R and best practice requirements;
- Ensure that the way we manage records is documented, understood and implemented; and
- Meet the reasonable current and future needs of internal and external stakeholders.

All electronic files retained on secure ATMOS Google cloud server.

Records that are no longer required are destroyed as soon as is practicable in an authorised and compliant manner.

2. Complaints

RECORD TYPE	EXAMPLES	RETENTION PERIOD	NOTES
Pupil/Public/Parent / Carer Complaint	Concerns Raised / Formal Complaint	3 years (From resolution of complaint plus time for leave to appeal).	In line with agreed R.E.A.L Complaints policy
External Agencies / Commissioners	In line with Service Level Agreements	3 years after agreement expires or is terminated.	

3. Properties, Equipment and Facilities

RECORDS TYPE	EXAMPLES	RETENTION PERIOD	NOTES
Equipment inspection records	PAT testing reports	5 years after equipment was replaced.	
Risk assessments	Fire risk assessments Method statements, general risk assessments	3 years or until superseded.	
Waste Management/ Confidential Waste Disposal	Disposal certificates, Waste recycling Agreements.	3 years.	
Building and engineering works	Surveys, site plans, bills of quantities, executed agreements, conditions of contract, specifications, “as built” record drawings Planning Consent Documents.	Lifetime of building occupancy.	The general principle to be followed in regard to these records is that they should be preserved for the life of the buildings and installations to which they refer.
Assets - Process of reporting and reviewing assets status	Routine returns and reports on asset status Inventories Stocktaking Disposal reports and proposals	2 years after administrative use is concluded.	

Inspection Reports – e.g. Boilers, Lifts, etc.		Lifetime of the installation.	Normally retain for the lifetime of an installation.
Property and Land Management			
Reports to management on leased/licenced and owned property	Consolidated property and buildings reports Summary of leased property Summary of owned property Site register Record of leases	Retain lifetime of tenure plus 36 months.	
Leases and Dilapidation reports		3 years from cessation of occupation.	
Memorandum of terms of occupation (Moto) agreements		Lifetime of building occupancy plus 3 years for final version.	
Management of the acquisition (by financial lease or purchase) process for real property		Retain for life of property or building plus 7 years.	

Management of the disposal (by sale or write off) process for real property	Legal documents relating to the sale Particulars of sale documents Board of survey	7 years after all obligations / entitlements are concluded.	
Title deeds and property related documents		Transfer to new owner on disposal	

4. Human Resources

RECORD TYPE	EXAMPLES	RETENTION PERIOD	NOTES
Disclosure of interests	Conflict of interest forms	7 years from the date of signing. All versions should be retained from date of signing, even if they have been superseded by a revised version incorporating changes.	All files held on ATMOS server and erased after retention period.
Statutory sick pay records, calculations, certificates and self certificates	Sickness absence monitoring reports	3 years after the end of the financial year to which they relate	

Statutory maternity: pay records, calculations, certificates Paternity and Parental leave, Adoption Leave, Special Leave, Unpaid Leave, & Career Break documents.		3 years after the end of the financial year to which they relate	
Disclosure and Barring registration documents (DBS)	Disclosure check,queries regarding DBS applications.	Destroy once concluded (maximum retention six months).	Police Act 1997 governs use of DBS checks
Recruitment of new employees.	Application forms, interview notes and reference details	3 years from the end of employment.	
Employee relations	Disciplinary details	Disciplinary details should be returned to HR for retention until the disciplinary action has expired. At expiry, the details will be destroyed. In any event, disciplinary details should be removed one year after employment has ended.	

Recruitment	Advertisements Applications Referee reports Assessment notes Feedback notes Interview reports Unsuccessful applicants	6 months after recruitment has been finalised.	Electronic and Paper
Monitoring staff performance	Probation reports Annual appraisal records	5 years after the action was completed.	
Employee File	Letter requesting clarification of terms/Role definition, Contract, evidence of identity	3 years from the end of employment.	
	References given/information to enable references to be provided	3 years from reference received/end of employment.	
	Summary of record of service, eg name, position held, dates of employment.	3 years from the end of employment.	
	Certificates Awards Exam results Qualifications	3 years from the end of employment.	

Termination	Resignation Redundancy (section 188) Dismissal Death Retirement	3 years after termination.	
Identification and development of significant directions concerning industrial matters	Generic agreements and awards Negotiations Disputes Claims lodged	Retain 5 years from termination.	
Liaison processes of minor and routine industrial matters	Daily industrial relations management	2 years after administrative use is concluded.	
Financial Reward	PAYE/salary documents. Jury service documents. P45. Overpayment and underpayment details. Westfield Health	7 years after action completed.	Archived, after 7 years electronic files erased.

Health and Safety

Reports	Accidents, incidents and near misses register. SIF	3 years from the date of last entry.	Reporting of Injuries, Disease and Dangerous Occurrences Regulations Reg 7;

On Site Checks	Audits, Monitoring forms Reports	3 years.	
PAT testing certificates	Annual	12 Months.	
Workstation Assessments. Occupational health referrals and proceedings Personal Injury information.		3 years after the end of the financial year to which they relate.	Keep any disputes on file until 3 years after termination.
Risk Assessments		Until reviewed and retained for 1 year.	

5. Information Systems & Information Communications Technology

RECORD TYPE	EXAMPLES	RETENTION PERIOD	NOTES
System documentation	Manuals, guides, build documentation, configuration documentation	Life of application or system plus six months.	
Asset Management	Inventory, including laptops, applications, software and licensing	Retain	Archived, after 3 years ATMOS server files erased.
IT asset Disposal Documents.		5 years	

Laptop and Mobile acceptance documents	Induction papers	On return of equipment.	
Laptop and Mobile return documents	Induction	One year from return.	
Office of Environmental Policy	Policy	Retain until superseded	
Performance information	Feedback	Delete upon analysis	
I.T. Helpdesk	Log of helpdesk calls	Retain	IT provider policy

6. Policies & Procedures

RECORD TYPE	EXAMPLES	RETENTION PERIOD	NOTES
Policy Documents	Internal policies	Retain until superseded	Review dates on document
	Internal procedures	Retain until superseded	
	Internal guidance	Retain until superseded	

7. Pupil/Learner Records

RECORD TYPE	EXAMPLES	RETENTION PERIOD	NOTES
"On-Roll" Pupil Files	Assessment / Annual/Academic Reports	End of Academic year of pupils 25th Birthday.	Archived, after spent all ATMOS server files erased.
Pupil Consent Forms	Consent pack	Duration plus 3 years.	
Pupil Work Folders	Work Packs	Duration.	To student at the end of term
Safeguarding Files	Electronic or Hard Copy Folders	Reviewed upon students 25th Birthday (see notes).	Reviewed after DofB +25 years and 2 yearly afterwards .
"Off Roll" Pupil Files	Pupil Folders	Duration of Placement / Assessment. (Term)	Files returned to the Commissioner at end of placement / Assessment on request. ATMOS server Files erased end each Term.
Looked after Students			
Safeguarding Files	Electronic or Hard Copy	Review file on a 5 year cycle or retain until Students 77th Birthday.	For "Off / Roll" learners file return to Commissioner end of placement.

END