R.E.A.L. Education Limited

General Data Protection Regulations, Practice and Procedure Policy

(R.E.A.L. Education Ltd.)
(R.E.A.L. Independent Schools, Hinckley)
(R.E.A.L. Independent Schools, Mansfield)

Last reviewed 12/02/2025

Contents

1. Policy

Aim

To ensure that confidentiality and Data Protection Compliance are a natural part of good practice.
To provide all staff and governors, unambiguous guidance as to their legal and professional roles.
To make certain that the procedures throughout R.E.A.L. can be easily understood by learners , parents/carers and staff.

Rationale

Schools hold a lot of confidential information about young people, staff and sometimes parents and carers. Whilst it is important that we continue to develop positive ways to use that information, we all recognise that it is our responsibility to use, hold and safeguard information received.

R.E.A.L. is mindful that they are placed in a position of trust and there is a general expectation that a professional approach will be used in all matters of confidentiality. Our obligation to comply with the Data Protection Act 2018, the UK GDPR and other legislation and statutory guidance underpins our management of data.

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 R.E.A.L. Education Ltd and R.E.A.L. Independent Schools (Hinckley,Mansfield), hereinafter referred to 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 for managing learner education and staff employment.

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 procedures 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 collects and processes. It also explains how we take care of data and what we do with the data once an individual leaves R.E.A.L (learner or

employee).

We want to make sure information about learners, parents/carers and staff is kept secure and within the law.

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. has a legal obligation to collect and process data in accordance with the UK 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 learners who are identified under two distinctive categories:

1. On roll learners - those young people who are registered as a learner at R.E.A.L Independent Schools (Hinckley, Mansfield).
2. Alternative Provision (AP) learners - those young people with R.E.A.L Education, on roll at another school or EOTAS, receiving alternative provision.

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.

Collect data for a specific purpose and use it for that purpose

Data cannot be used for a purpose that it was not originally collected for, or where notice has not been given about how data may be used after collection.

Limited collection

Data Controllers should only collect the minimum amount of data needed for a particular task or reason. If there is a breach or a hack only limited information can be lost.

Accuracy

Data collected should be accurate, and steps should be taken to check and confirm accuracy. This is done when learners join the school and is reviewed on an annual basis. If a Data Subject feels that the information held is inaccurate, should no longer be held by the Controller or should not be held by the Controller in any event, a dispute resolution process and complaint process can be accessed, using the suitable forms. An approach should be made directly to the Data Protection Officer (DPO) at R.E.A.L.

Individual Rights

The GDPR provides eight key principles in ensuring the rights for data subjects, 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’, this can be found on our websites.

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. 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

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., are deemed the 'controllers' and have overall responsibility for this policy.
3. A **processor** is responsible for processing personal data on behalf of the controller. All staff at R.E.A.L are deemed as 'processors'.
4. The centralised services within R.E.A.L.(HR, and financial services) are also deemed as the data processors on behalf of R.E.A.L.
5. Educational services (alternative provision) provided through R.E.A.L Education are 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 third party 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 – e.g. 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 information that we collect/hold on our workforce, learners and parents/carers and who we share data with, is detailed in the Privacy Notices available on the website.

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).

CCTV

Some of the schools within the R.E.A.L. use CCTV. The use of CCTV and storage of images for a period of time is in line with UK GDPR.

CCTV may be used for:-
• Detection and prevention of crime
• School staff disciplinary procedures
• Learner behaviour management processes
• To assist the school in complying with legal and regulatory obligations

2. Procedure

Data Storage and Security

We have processes in place to keep data safe. That might be paper files, electronic records or other information.

Electronic Storage. All information is stored on the R.E.A.L. Google Drive with password protections and 2 step verification in place or password protected web based platforms.

Physical Security. On all our sites staff are responsible for ensuring that the space is securely maintained and controlled if unoccupied, i.e. locked. Offices and cupboards that contain personal data should be secured at all times. All staff, contractors and third parties who have control over lockable areas must take due care to prevent data breaches. All sites and locations need to have the suitable security and review measures in place.

Secure Disposal. When disposal of items is necessary a suitable process must be used. This is to secure the data, to provide a process that does not enable data to be shared in error, by malicious or criminal intent. These processes, when undertaken by a third party are subject to contractual conditions to ensure UK GDPR and DPA compliance.

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.

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. If a learner leave mid 'school life cycle' files for on roll learners are transferred to the new School
3. Records for Alternative Provision (AP) learners are only kept until the end of the academic year 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, if requested, at the end of the placement and deleted from google drive at the end of the academic year. Minimal data (name, DOB, placement dates, qualification details) are kept to allow R.E.A.L Education to fulfil its obligations for educating, processing and reporting.

Data Subject Access Request 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 any format, writing; which includes email or phone call to any member of R.E.A.L Education staff. . All requests will be sent to the DPO immediately.

3. The DPO will send the requestor a form to complete for further information, establishing identity 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 Learning Manager 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 with our Legal GDPR Advisors.

Data Breaches

The GDPR introduces a duty on all organisations to report certain types of personal data breach to the relevant supervisory authority.

All members of staff are required to familiarise themselves and comply with R.E.A.L. GDPR policy and procedures. Training will be provided to all staff to enable them to carry out their obligations within this policy.

At R.E.A.L staff are required to inform the DPO immediately on discovery of a breach. Breaches will be reported to the ICO 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 or most appropriate person i.e. the Learning Manager, HR, will inform those individuals without undue delay by phone.

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, Head of Business Operations 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.

We will describe, in clear and plain language, the nature of the personal data breach and, at least:

- the name and contact details of any data protection officer you have, or other contact point where more information can be obtained;
- a description of the likely consequences of the personal data breach; and
- a description of the measures taken or proposed to deal with the personal data breach and, where appropriate, a description of the measures taken to mitigate any possible adverse effects.

When reporting a breach to the ICO we will provide the following information:

- a description of the nature of the personal data breach including, where possible:
    - the categories and approximate number of individuals concerned; and
    - the categories and approximate number of personal data records concerned;
- the name and contact details of the data protection officer (if your organisation has one) or other contact point where more information can be obtained;
- a description of the likely consequences of the personal data breach; and

- a description of the measures taken, or proposed to be taken, to deal with the personal data breach and, where appropriate, of the measures taken to mitigate any possible adverse effects.

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.

Record of Processing of Activities (RoPA)

Our RoPA document helps us to ascertain what documents and systems are used within R.E.A.L. to store and process personal information. This document is updated as and when changes happen but also reviewed on an annual basis, by the DPO, to ensure accuracy.

3. Practice

The Data Protection Officer

The GDPR introduces a duty for you to appoint a data protection officer (DPO) 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. and the School Governors.
- 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.

Appendix A

GDPR: Information Security Protocol – all staff and governors

Introduction

Information security is everyone's responsibility. Personal and sensitive data is used, stored, shared, edited and deleted everyday by everyone in R.E.A.L. Education.

This protocol applies to all staff (which includes governors, agency staff, contractors, work experience students/teachers) when handling personal and sensitive data.

This protocol explains responsibilities that are already part of contracts of employment, our voluntary agreements and reflect relevant statutory responsibilities.

The data protection policy sets out how our statutory obligations are managed. Details of how personal data is used is contained within privacy notices. More details about individual's rights, information management and other protocols are on the website.

Day-to-day data handling

You must be aware of data protection and privacy whenever you are handling personal and sensitive data.

Data protection is about looking after information about individuals.

Personal data

Personal data can be a name, address, or other identifier, for example a national insurance number. These are also identifiers.

It is usual for other information to attach to the identifier. This may be attainment and progress data for a pupil. It could be details of which sport teams they play for. Details of parents/carers and contact information.

Staff examples include CPD records, performance management information, next of kin details. These are just a few examples of personal data.

Sensitive personal data

However, some personal data is more sensitive. This is called sensitive personal data in this policy and in the data protection policy. Greater care about how that data is used is required.

Sensitive personal data is:

- information concerning safeguarding and child protection matters
- information about serious or confidential medical conditions and information about special educational needs
- information concerning serious allegations made against an individual (whether or not the allegation amounts to a criminal offence and whether or not the allegation has been proved)
- financial information (for example about parents and staff)
- information about an individual's racial or ethnic origin
- political opinions
- religious beliefs or other beliefs of a similar nature
- trade union membership
- physical or mental health condition
- genetic information
- sexual life or sexual orientation
- information relating to actual or alleged criminal activity
- biometric information (e.g. fingerprints used for controlling access to a building)

Staff need to be extra careful when handling sensitive personal data.

Minimising the amount of personal data that we hold

Restricting the amount of personal data we hold, to that which is needed, is to help keep personal data safe. You should never delete personal data unless you are sure you are allowed to do so. If you would like guidance on when to delete certain types of information, please check the retention schedule and/or take advice from the DPO.

What is an information security breach?

Sometimes, things go wrong. If you think or know that something has gone awry, it is critical that this is reported to the DPO immediately by phone and email.

Information security breaches can happen in a number of different ways. Examples include:

- sending a confidential email to the wrong recipient

- letters sent to the wrong address with health and SEN data included
- overhearing conversations about a member of staff's health
- a laptop / phone stolen after being left in a car
- hacking of school systems
- leaving confidential documents containing personal data in a car that was stolen

These are examples of personal data breaches. They all need to be reported to the R.E.A.L. Education Data Protection Officer.

This includes anything which you become aware of even if you are not directly involved (for example, if you know that document storage rooms are sometimes left unlocked at weekends).

The sooner a breach is notified to the right person, the sooner and more effectively it can be managed.

In certain situations, it is necessary to report a breach to the Information Commissioner's Office (the data protection regulator) and let those whose information has been compromised know within strict timescales. This is another reason why it is vital that we report breaches immediately.

Basic IT expectations

Lock computer screens: Your computer screen should be locked when it is not in use, even if you are only away from the computer for a short period of time.

If you are not sure how to do this, then speak to IT.

Be familiar with the tech: You should also make sure that you familiarise yourself with any software or hardware that you use. In particular, please make sure that you understand what the software is supposed to be used for and any risks.

For example:

- Compass/ CPOMS – make sure that students cannot see personal data of other Learners
- be careful when casting your screen / logging onto smartboards in classrooms, that you are not oversharing information
- you need to be extra careful where you store information containing sensitive personal data. Ensure documents are stored on ATMOS drive or CPOMS with the agreed sharing protocols

Portable media devices

The use of portable media devices (such as USB drives, portable hard drives, DVDs) is not allowed unless those devices have been given to you by R.E.A.L. Education and you have received training on how to use those devices securely. The IT team will provide guidance about protect any portable media device given to you with encryption.

Hardware and software provided by R.E.A.L. Education.

IT equipment provided by R.E.A.L Education (this includes laptops, chromebooks and phones) is recorded on the IT equipment asset register. All equipment must be used as per the R.E.A.L Technology Agreement: Mobile Phone / Laptop / Chromebook / Vehicles . Equipment must always be returned to the Head Office even if you think that it is broken and will no longer work, and the asset register updated accordingly.

Where to store electronic documents and information

You must ensure that you only save or store electronic information and documents in the correct location on R.E.A.L. Education ATMOS drive or CPOMs system, with the correct sharing permissions. Do not save information on desktops or local drives.Storage of information should follow the guidance in the R.E.A.L. ICT data process and storage statement for staff

Passwords

Passwords should be long and difficult to guess, for example, you could use a song lyric or a memorable phrase plus a number. Do not choose a password which is so complex that it's difficult to remember without writing it down. Your password should not be disclosed to anyone else.

You should not use a password which other people might guess or know, or be able to find out, such as your address or your birthday.

You must not use a password which is used for another account. For example, you must not use your password for your private email address or online services for any school account.

Passwords (and any other security credential you are issued with such as a key fob or USB drive) must be kept secure and confidential and must not be shared with, or given to, anyone else. Passwords should not be written down.

Emails

When sending emails, you must take care to make sure that the recipients are correct. The most common source of R.E.A.L. Education data breaches are emails sent to the wrong person or sent CC not BCC.

Emails to multiple recipients

When sending a group email, please take time to check the recipients carefully. If you have group email names, are they easy to see on devices? Is it possible to choose the wrong email group if you are in a rush? Should the group be renamed? For example, any group to staff should begin with ‘STAFF’ and then a description.

If you are selecting recipients, take a moment to check that these really are the people you want to share data with.

If the email contains sensitive personal data, then you should consider how to protect it whilst in transit.

Encryption

Remember to encrypt internal and external emails which contain sensitive personal data. For example, Word documents can be attached to email and encrypted with a password which can then be forwarded separately to the recipient.

Private email addresses: You must not use a private email address for school related work. You must only use your official email address. Please note that this rule applies to governors as well.

Paper files

Keep under lock and key: Staff must ensure that papers which contain sensitive personal data are properly secured. This is likely to require a lockable, secure location and that they are never left unattended on desks (unless the room is secure). Any keys must be kept safe.

If the papers contain sensitive personal data, then they must be kept in secure cabinets. Information held in paper form must not be stored in any other location, for example, child protection information should only be stored in the cabinet managed by the Designated Safeguarding Lead (DSL) and Deputy Designated Safeguarding Lead's.

Disposal

Paper records containing personal data should be disposed of securely. Make sure that such material is either shredded onsite or handed to the receptionist to do this or large volumes of paperwork for disposal can be sent to Head Office and confidential disposal collections can be arranged. **Personal data should never be placed in the general waste.**

Printing

When printing documents, make sure that you collect everything from the printer at the time of printing, otherwise there is a risk that confidential information might be read or collected by

someone else. If you see anything left by the printer or comes out of the printer when you print take it to the receptionist or Site lead for immediate disposal.

Put papers away

Papers should be stored in an appropriate location onsite, check with the site responsible people.

Post

Caution is to be applied when sending items in the post. Confidential materials should not be sent using standard post. Signed for or guaranteed delivery are options to be used. However, do consider using secured email as an option.

Working off-site (e.g. R.E.A.L. Education trips and home working)

Personal and sensitive data is taken off site for many reasons. For example, because a staff member is working from home or supervising a trip.

This does not breach data protection law if appropriate safeguards are in place to protect the data.

For trips, the trip organiser should decide what information needs to be taken and who will be responsible for looking after it.

When working from home is it necessary to apply the same security measures as if on site. Sensitive personal data must be properly secured and dealt with the same diligence as when onsite.

Take the minimum with you

When working away from sites you must only take the minimum amount of information with you. For example, a teacher organising a field trip might need to take with her information about pupil medical conditions (for example allergies and medication). If only two out of a group of six learners are going offsite, then the Lead staff member should only take the information about the two pupils.

Confidential wallets will be available for all Managers to use in order to take personal data paperwork off site.

Working in the community

You must not work on documents containing personal and sensitive data whilst in the community, or travelling by train, if there is a risk of unauthorised disclosure (for example, if there is a risk that someone else will be able to see what you are doing). For example, if working on a laptop in a cafe or Library you should ensure that no one else can see the laptop screen and you should not leave any device unattended where there is a risk that it might be taken.

Paper records

If you need to take hard copy records with you then you should make sure that they are kept secure.

For example:

- documents should be kept secure at all times if left unattended
- when travelling by car, you must keep the documents out of plain sight. Please be aware that possessions left on car seats are vulnerable to theft when your car is stopped
- if you have a choice between leaving documents in a vehicle and taking them with you (e.g. to a meeting) then you should take them with you and keep them secure

Hardware and software not provided by R.E.A.L. Education.

Staff must not use any device or software that is not owned and managed by R.E.A.L. education unless permission is given by HR and the DPO.

Sending or saving documents to your personal devices

Documents containing personal and sensitive data (including photographs and videos) ***should not*** be sent to or saved to personal devices unless you have been given permission by the DPO This is because anything you save to your computer, tablet or mobile phone will not be protected by R.E.A.L. Education. security systems.

Furthermore, it is often very difficult to delete something which has been saved to a personal device or computer.

For example, if you saved a school document to your laptop because you wanted to work on it over the weekend, then the document would still be on your computer hard drive even if you deleted it and emptied the recycle bin.

Friends and family

If you have been given permission to use your device for work you must take steps to ensure other people (family and friends) can not access any R.E.A.L documents that may be on your device.

Breach of this protocol

Any breach of this protocol will be taken seriously and may result in disciplinary action.

A member of staff who deliberately or recklessly obtains or discloses personal and/or sensitive data held by R.E.A.L. Education without proper authority may also be guilty of a criminal offence and gross misconduct. This could result in dismissal.

This protocol does not form part of any employee's contract of employment.

We reserve the right to change this protocol at any time. Where appropriate, we will notify staff of those changes by mail or email.

Appendix B

Data Deletion and Retention Policy.

Contents

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 a secure Google cloud server. Paper records are stored in securely locked storage areas on R.E.A.L Education sites or an offsite secure storage facility.

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
Learner/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 leased property Summary 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.

5. Health and Safety

RECORD TYPE	EXAMPLES	RETENTION PERIOD	NOTES
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.	

6. 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.	
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

7. 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	

8. Learner Records

RECORD TYPE	EXAMPLES	RETENTION PERIOD	NOTES
“On-Roll” Learner Files	Electronic files or hard copy folders containing Assessments / EHCP/Academic Reports/Consent Forms Previous School files	End of Academic year of learners 25th Birthday.	After spent all Google server files erased and paper files confidentially destroyed
“On-Roll” Learner Work Folders	Student work google file Paper academic work box files	Duration plus 1 year	Qualification work retained under individual exam board requirements
Safeguarding Files for on roll and Alternative Provision (AP) Learners	Electronic files or hard copy folders and CPOMS records	Reviewed at the end of Academic year upon students 25th Birthday (see notes).	Reviewed after DofB +25 years and 2 yearly afterwards .
“Alternative Provision (AP)” Learners Files	Learner Folders	Duration of Placement	On request files returned to the Commissioner at end of placement. Google server files erased at the end of each academic year.

"Alternative Provision (API" Learner Work Folders	Student work google file Paper academic work box files	Duration of placement	On request work returned to the Commissioner at end of placement.
Qualification Course work for on roll and Alternative Provision (AP) Learners	AIM Awards Functional Skills BTEC GCSE Vocational Qualifications	In line with exam board requirements	
Looked after Students			
Safeguarding Files	Electronic or Hard Copy	Review file on a 5 year cycle or retain until Students 77th Birthday.	

9. Emails / Text messages

RECORD TYPE	EXAMPLES	RETENTION PERIOD	NOTES
Emails	Any email on a @real-education.org account	Under review	
Text Messages	Any text messages on a phone account allocated to R.E.A.L. Education	Under review	