R.E.A.L Education

Re-thinking Engagement & Approaches to Learning

Data Protection and Processing Policy (R.E.A.L. Education Ltd.)

Amended on: 21.12.16

Review Date: January 2018

Revision history:

Version 1	Completed 11 April 2014 and shared with ICT Strategy group
Version 2	Added section on Data loss and destruction and changed format to standardised R.E.A.L. format. 11.1.16
Version 3	Annual update completed by Craig Wilkie 21.12.16 Minor updates and amendments.

Contents

- What is the purpose of this policy?
- Introduction
- Collecting data
- Processing of data
- Data loss or destruction
- Sharing of personal data
- Requesting data held by R.E.A.L. Education / Freedom of Information request
- Updating of policy
- Addressing complaints
- Further information and Contacts

What is the purpose of this policy?

This policy outlines what types of data R.E.A.L. Education collects and processes. It explains how we take care of data and what we do with your data when a young person leaves 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 Data Protection Act 1998.

It is the responsibility of the Directors, Head of Business Services and Head of ICT Services to develop and review this policy.

This policy adheres to the requirements of the act.

Introduction

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, Groups provisions and other activities

delivered by R.E.A.L. LTD.

We use the term data processing to cover the gathering, ordering, storing, transport and disposal of data.

We acknowledge that R.E.A.L. Education 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. Education 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.

Collecting data

We collect data, including personal and sensitive personal data. Personal data is that which can be used or combined to identify a living person. The data types we collect are exemplified in the table below:

Personal data	Sensitive personal data
• Name • Age / Date of birth • Address • Schools attended	• Medical information / Health • Statement / EHC plan • Organisations/Support services involved in a young person's care

We will only collect data which is:

- Relevant to the services and care we are providing to a young person and their family
- Non-excessive, providing the minimum quantity and depth of data as is required to deliver our services.

We will be transparent about our data policy from the outset, by providing all students and/or their parents/carers with our Privacy Notice. This takes the form of the “R.E.A.L. ICT data process and storage statement, agreement for parents and students”. The Information Commissioner would describe this as the Privacy Notice.

REAL, ICT data process and storage statement, agreement for parents and students

Example requiring a signature
https://docs.google.com/a/real-education.org/document/d/1tVl8XysUn3juRQDhRpk9Yk2PMGselGwGr2IE2GcU1Vk/edit?pli=1

OR

Example of a Privacy leaflet (not requiring a signature)
https://docs.google.com/document/d/1S9m-sindKx1JUmId_TjDIwx7uFJisSm6R9muivykiXw/edit

Examples of the student data we collect

The following examples highlight the types of student data we collect and the reasons for collection. This is not an exhaustive list, but demonstrates the breadth of information we collect and process at R.E.A.L. Education.

A tutor is asked by the office to pick up a child from their home. They access a computer record

which tells them the address of the child so they are able to pick them up.

A range of tutors are writing the end of year report. They each complete their section of the report and email this back to the school office. The report is shared between all tutors so they are able to understand how the student is progressing across the curriculum.

A new tutor is working with a child. She/He accesses a computer record for the child to be aware of any medical conditions such as allergies as they are about to go to a Cafe to do some work experience.

A teacher takes a photo of a piece of artwork or activity and saves this to a student's computer, the student is distinguishable in the photograph. Permission has been granted by the student and their parents at induction and again, verbally before the photograph is taken.

Processing of data

We recognise that as an education provider, it is essential to have access to a range of data about young people.

We use the term data processing to cover the gathering, ordering, storing, transport and disposal of data.

We process data, adhering to the following principles:

Personal data will be processed fairly and lawfully

- we will have legitimate grounds for collecting and using the personal data;
- we will not use the data in ways that have unjustified adverse effects on the individuals concerned;
- we will be transparent about how we intend to use the data, and give individuals appropriate privacy notices when collecting their personal data;
- we will handle people's personal data only in ways they would reasonably expect
- we will make sure we do not do anything unlawful with the data eg, share data without prior consent (except where we are legally enforced to do so).

Personal data shall be accurate and kept up to date

- we will routinely ask parents to confirm the data we hold is accurate.
- we ask parents/staff to tell us when information changes eg. change of address, so we can keep our record accurate.

Personal data should be kept for no longer than necessary

- We are required to store some data about students after they have left R.E.A.L. Education eg. to report on anonymised academic performance, progress reports, in order to give references to future employers/educational establishments, consent forms to prove we sought consent to take a photograph which was used in our Newsletter.
- Information considered non-relevant to anticipated future requests will be removed from our electronic records within a reasonable period of time after the leaving date of a pupils/staff member unless specific consent is gained for a specific purpose. Non-relevant data will include Statement/EHC plan, risk assessments. In the case of staff leaving R.E.A.L., this will include information such as bank account details.

R.E.A.L. Education will take organisational and technical measures against unauthorised access and loss, damage and destruction of personal data.

- Personal data is managed through the use of the Google Atmos document storage system. The Business team provides access to Learning Managers and Group Leaders to the information required in order to care and educate a student. Access to data by individual tutors is managed and coordinated by the Learning Manager/Group Leader.
- Password protection is required on all devices used to access personal information such as a phone or laptop.
- Password protection is used when accessing all data on the Google/Atmos document storage system.
- Two step verification is used to provide enhanced security.
- Where a password is compromised the Business Team at Castledine House will be contacted immediately and the account will be secured by the IT team.
- (Applies to non-Business team staff only) Personal information in a digital format will not be downloaded to hardware, rather accessed through the Google / Atmos system to ensure no personal data exists on the hard drive of a device.
- Personal data will not be carried on portable storage equipment eg. memory sticks or hard drives.
- We will routinely educate and support staff to keep data safe in electronic systems eg. signing out of systems, changing password, choosing strong passwords etc…including offering eSafety and Data Protection advice at induction.
- We won't store a record of passwords and usernames for the Google / Atmos system for staff or students, to ensure the integrity of the system.
- When staff leave R.E.A.L. Education, we will disable the access to systems to ensure that data cannot be accessed at a later date.
- When data is misplaced or destroyed accidentally, we will inform the Data Commissioner and seek advice about the steps required to inform those who may be affected from a

breach of our Data policy.
- Where IT systems and equipment is decommissioned, we will work with partners to ensure data is correctly destroyed and erased before destruction/recycling of the equipment.

Personal data will be processed in accordance with the rights of data, subject to the data protection act.

- We process all data with regard to the Data Protection Act.
- We are registered with the Data Commissioner to demonstrate our commitment to collecting and processing data with care and consideration.

Personal data should not be transferred outside European Economic Area unless that country has adequate levels of protection for rights and freedoms of data.

- All data saved to the Google / Atmos system is encrypted and stored in data centres in the EEA (European Economic Area) and to other locations legally protected by the Safe Harbour Agreement. This ensures that data is subject to the same security and protections as afforded to data stored within EEA.
- Data stored off-site (not on a R.E.A.L. premises) in the Google / Atmos cloud is afforded one of the most comprehensive security processes available today - by dissecting, encrypting and physically separating files into different data centres, thus providing excellent resilience and security protections beyond what could be achieved by R.E.A.L.s internal ICT support services.
- We back-up our data in a similar way, using approved Google Apps providers, thus ensuring data and business continuation in the unlikely event of a total systems failure of the Google Apps system.

Data loss or destruction

At R.E.A.L. we recognise that a data breach is a possibility and plan for the action we would take if this event occurred.Where confidential data is lost (including stolen) or destroyed we will implement the following process in line with guidance from the Information Commissioner.

There are four important elements to any 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 Directors must be informed and depending on the nature of the data - the ICT Team will be informed through www.realservicedesk.co.uk
2. Assessing the risks – The ICT Strategy group and Directors will assess any risks associated with the breach, as these are likely to affect the actions we take once the breach has been

contained. In particular, we will assess 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. Directors will decide who needs to be notified and why. You should, 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 – Directors will investigate the causes of the breach and also evaluate the effectiveness of the response to it. If necessary, the Directors will request an update to policies and procedures.

Sharing of personal data

Sharing personal student data within R.E.A.L. Education
Data stored using IT is shared through a controlled system, using the Google / Atmos system.

Personal student data is not shared with staff unless there is a clear reason to do so.

On induction, we establish the right to collect and process personal data within R.E.A.L. Education from the student and/or parents.

All student personal data is accessible to the Business Team in R.E.AL. Education and theoretically accessible by the ICT technical services provider (eLearning team) who manage and maintain ICT systems. All eLearning team staff have signed a legally enforceable order, meaning civil/criminal action could be taken if any data is accessed without permission from R.E.A.L. Education. All eLearning team staff hold clean, enhanced CRB/Disclosure and Barring certificates.

Sensitive Personal data is initially accessible to the Business Team and the Learning Manager / Group Manager with responsibility for the young person.

Access to Sensitive Personal information is delegated to Tutors via the Learning Manager / Group Manager on a file by file basis.

Access to Personal information is delegated to Tutors via the Learning Manager / Group Manager through access to a shared folder where any new documents placed in the folder are accessible to the Tutor's who have been granted access.

The Learning Manager and Group Leader holds the responsibility to ensure that tutor/other staff access to personal student data is routinely audited and adjusted. This ensures that only those who have a legitimate reason to access student personal information are able to do so.

Sharing personal data outside of R.E.A.L. Education

We will only share personal information with parties outside of R.E.A.L. Education when it is legally appropriate or where we are legally enforced to do so.

In this case, we inform individuals when their information is shared, and why and with whom it was shared.

Example situations where we will share data.

A student's prospective employer / education establishment requests a reference. We will check with the student to confirm the authenticity of this request. The student has a right to request access to the reference.

The school where the student is on roll requests a progress report on the student's academic performance at R.E.A.L. Education. The **REAL, ICT data process and storage statement, agreement for parents and students** gains the authority to share this information with the roll school. R.E.A.L. Education staff are able to send the progress report to the roll school, after ensuring the request is legitimate and personnel have the delegation to request the information.

R.E.A.L. Education publishes a performance table of academic qualifications gained by students over the academic year. This information is anonymised and aggregated, it is not personal information as it would be impossible to identify the student from the aggregated data. Request to publish this information does not need to be gained from the student.

A parent requests information about their child's academic performance. The Business Team must verify that this is the parent of the child and has permission to request the information.

The default position at R.E.A.L. Education is to routinely seek parental/student permission before personal data is shared with people outside of R.E.A.L. Education. That this information is shared in a way which ensures the integrity of the data and that it can be delivered in a secure way to the data requester.

Requesting data held by R.E.A.L. Education / Freedom of Information request

This section of our policy outlines the procedures for responding to subject access requests made under the Data Protection Act 1998 and has been adapted from guidance provided by Essex County Council to schools and academies.

Rights of access to information
There are two distinct rights of access to information held by schools about pupils.

1. Under the Data Protection Act 1998 any individual has the right to make a request to access the personal information held about them.

2. The right of those entitled to have access to curricular and educational records as defined within the Education Pupil Information (Wales) Regulations 2004.

These procedures relate to subject access requests made under the Data Protection Act 1998.

Actioning a subject access request
1. Requests for information must be made in writing; which includes email, and be addressed to Brian Smith, Director of R.E.A.L. Education. If the initial request does not clearly identify the information required, then further enquiries will be made. (enquiries@real-education.org)
2. The identity of the requestor must be established before the disclosure of any information, and checks should also be carried out regarding proof of relationship to the child. Evidence of identity can be established by requesting production of:

- passport
- driving licence
- utility bills with the current address
- Birth / Marriage certificate
- P45/P60
- Credit Card or Mortgage statement

This list is not exhaustive.

3. Any individual has the right of access to information held about them. However with children, this is dependent upon their capacity to understand (normally age 12 or above) and the nature of the request. The Director of R.E.A.L. Education should discuss the request with the child and take their views into account when making a decision. A child with competency to understand can refuse to consent to the request for their records. Where the child is not deemed to be

competent an individual with parental responsibility or guardian shall make the decision on behalf of the child.

4. The school may make a charge for the provision of information, dependant upon the following:

Should the information requested contain the educational record then the amount charged will be dependant upon the number of pages provided.

Should the information requested be personal information that does not include any information contained within educational records schools can charge up to £10 to provide it.

If the information requested is only the educational record viewing will be free, but a charge not exceeding the cost of copying the information can be made by the Director of R.E.A.L. Education.

5. The response time for subject access requests, once officially received, is 40 days (not working or school days but calendar days, irrespective of school holiday periods). However the 40 days will not commence until after receipt of fees or clarification of information sought

6. The Data Protection Act 1998 allows exemptions as to the provision of some information; therefore all information will be reviewed prior to disclosure.

7. Third party information is that which has been provided by another, such as the Police, Local Authority, Health Care professional or another school. Before disclosing third party information consent should normally be obtained. There is still a need to adhere to the 40 day statutory timescale.

8. Any information which may cause serious harm to the physical or mental health or emotional condition of the pupil or another should not be disclosed, nor should information that would reveal that the child is at risk of abuse, or information relating to court proceedings.

9. If there are concerns over the disclosure of information then additional advice should be sought.

10. Where redaction (information blacked out/removed) has taken place then a full copy of the information provided should be retained in order to establish, if a complaint is made, what was redacted and why.

11. Information disclosed should be clear, thus any codes or technical terms will need to be clarified and explained. If information contained within the disclosure is difficult to read or illegible, then it should be retyped.

12. Information can be provided at R.E.A.L. Education with a member of staff on hand to help and explain matters if requested, or provided at face to face handover. The views of the applicant should be taken into account when considering the method of delivery. If postal systems have to be used then registered/recorded mail must be used.

Complaints

Complaints about the above procedures should be made to the Chairperson of the Governing Body (contactable through enquiries@real-education.org) who will decide whether it is appropriate for the complaint to be dealt with in accordance with the R.E.A.L. Education's complaint procedure. Complaints which are not appropriate to be dealt with through R.E.A.L. Education's complaints procedure can be dealt with by the Information Commissioner. Contact details of both will be provided with the disclosure information.

Contacts

If you have any queries or concerns regarding these policies / procedures then please contact Brian Smith, Director of R.E.A.L. Education (enquiries@real-education.org)

Further advice and information can be obtained from the Information Commissioner's Office, www.ico.gov.uk

---

Updating of policy

This policy will be reviewed as it is deemed appropriate, but no less frequently than every year.

The policy review will be undertaken by the ICT Strategy group and presented to the Director of R.E.A.L. Education, or nominated representative.

Addressing complaints

Complaints will be dealt with in accordance with the R.E.A.L. Education's complaints policy. Complaints relating to information handling may be referred to the Information Commissioner (the statutory regulator).

Further information and Contacts

If you have any enquires in relation to this policy, please contact

The Business Manager, Castledine House, 7 Heanor Road, Ilkeston, Derbyshire, DE7 8DY who will also act as the contact point for any subject access requests.

Further advice and information is available from the Information Commissioner's Office, www.ico.gov.uk or telephone 01625 5457453

END