Freedom of Information & Data Protection Policy and Procedure

Audience:	All staff, governors, agency staff, contractors, work experience students and volunteers
Approved:	Jan 2022
Other related policies:	Information Security Policy
Policy owner:	Director of HR
Policy model:	
Review:	Oct 2022
Version number:	1.0

Freedom of Information and Data Protection Policy and Procedure

At REAch2, our actions and our intentions as school leaders are guided by our Touchstones

Integrity

We recognise that we lead by example and if we want children to grow up to behave appropriately and with integrity then we must model this behaviour

Responsibility

We act judiciously with sensitivity and care. We don't make excuses, but mindfully answer for actions and continually seek to make improvements

Inclusion

We acknowledge and celebrate that all people are different and can play a role in the REAch2 family whatever their background or learning style

Enjoyment

Providing learning that is relevant, motivating and engaging releases a child's curiosity and fun, so that a task can be tackled and their goals achieved

Inspiration

Inspiration breathes life into our schools. Introducing children to influential experiences of people and place, motivates them to live their lives to the full

Learning

Children and adults will flourish in their learning and through learning discover a future that is worth pursuing

Leadership

REAch2 aspires for high quality leadership by seeking out talent, developing potential and spotting the possible in people as well as the actual

Freedom of Information and Data Protection Policy and Procedure

Contents

1. Purpose

The purpose of this policy and procedure is to ensure compliance of REAch2 Academy Trust ("the Trust" which means the Trust and its academies) with all of its obligations as set out in the Data Protection and Freedom of Information legislation encompassed under the General Data Protection Regulations.

2. Data Controller

The Trust is the Data Controller as defined in the General Data Protection Regulations 2018.

3. Notification with the Information Commissioner's Office (ICO)

3.1 The Trust notified the ICO, when it was established, using the on- line form. Under the new GDPR regulations this registration is renewed annually.

3.2 The Trusts registration is: ZA075052,

3.2 The Trust will renew the registration annually and is due on 9th October 2021. In addition, if the Academy introduces any new purposes for processing personal information, such as the installation of CCTV, then it will undertake a Data Protection Impact Assessment on the new installation.

4. Definitions

4.1. **Personal data** is information that relates to an identifiable living individual that is processed as data. Processing means collecting, using, disclosing, retaining, or disposing of information. The data protection principles apply to all information held electronically or in structured files that tells you something about an identifiable living individual. The principles also extend to all information in education records. Examples would be names of staff and pupils, dates of birth, addresses, national insurance numbers, school marks, medical information, exam results, SEN assessments and staff development reviews.

4.2. **Sensitive personal data** is information that relates to race and ethnicity, political opinions, religious beliefs, membership of trade unions, physical or mental health, sexuality and criminal offences. There are greater legal restrictions on processing sensitive personal data than there are on personal data.

5. Data Protection Principles

- The new GDPR regulations set out principles for the processing of personal data, the rights of individuals to access data, and tighter regulations for how breaches must be dealt with.
- These say that personal data must be:
- Processed lawfully, fairly and in a transparent manner
- Collected for specified, explicit and legitimate purposes
- Adequate, relevant and limited to what is necessary in relation to the purposes for which the data is processed
- Accurate and kept up to date
- Kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the data is processed
- Processed in a way that ensures appropriate security

6. Fair Processing

6.1 The Trust is committed to being clear and transparent about what type of personal information we hold and how it is used. The Trust has separately published its 'Privacy Notice for Parents and Pupils' and "Privacy Notice for Employees" which both are available on the Trust's Web Site.

7. Privacy Notice for Parent and Pupils and Privacy Notice for Employees

7.1 The Privacy Notices are intended to provide information about how the Trust and its academies will use, or 'process', personal data about individuals including: its current, past and prospective pupils and their parents, carers, guardians or wider family members (for instance siblings or other extended family members who may be named as emergency contacts) - referred to in this notice as 'parents'.

7.2 Personal information is information that identifies an individual as a person and which relates to them as an individual. This makes the Trust a data controller of this personal information, and the Privacy Notices sets out how we will use that information and what the individual's rights are. Parents are encouraged to read the published Privacy Notice and understand the Trust's obligations.

Similarly, the Privacy Notice for employees explains how and why we collect personal information about our employees and what we do with that information. It also explains the decisions that employees can make about their own information. Employees are encouraged to read the published Privacy Notice.

7.3 The Privacy Notices applies alongside any other information the Trust may provide about a particular use of personal data, for example when collecting data via an online form, or images captured on closed circuit television (CCTV).

7.4 The Privacy Notices applies in addition to the academy's other relevant policies, including REAch2's policy on information security and records retention,

safeguarding, pastoral, or health and safety policies and IT policies.

7.5 Anyone who works for, or acts on behalf of, the academy, including staff, volunteers, governors and service providers, should also be aware of and comply with the respective Privacy Notices and the Trust's data protection policy for staff, which provides further information about how personal data on those individuals will be used.

8. Information Security

8.1 Overarching Principles

Information security is about what you and the Trust do to ensure that Personal Data is kept safe. This policy provides guidance on how we protect data to ensure the Trust meets the requirements of the Data Protection Act and the General Data Protect Regulations (GDPR) and to give reassurance to those who entrust their data with us.

8.2 Responsibilities

The Trust is responsible for how all staff and anyone who works for, or on behalf of, the Trust handle personal information. In this policy, the term 'Trust' applies to all REAch2 academies and this policy applies to all staff, including governors, agency staff, contractors, work experience students and volunteers.

For more information on what Personal Data is, refer to the Trust's Data Protection Policy.

8.3 General Security

This policy meets the requirements of the Data Protection Act and the GDPR and is based on guidance published by the Information Commissioner's Office (ICO).

8.1.1. It is important that unauthorised people are not permitted access to Trust information and that we protect against theft of both equipment and information. This means that we must pay attention to protecting our buildings against unauthorised access. Staff must:

8.1.2. Not reveal pin numbers or building entry codes to people that you do not know or who cannot prove themselves to be employees;

8.1.3. Beware of people tailgating you into the building or through a security door;

8.1.4. If you don't know who someone is and they are not wearing some form of identification, ask them why they are in the building;

8.1.5. Not position screens on reception desks where members of the public could see them;

8.1.6. Lock secure areas when you are not in the office;

8.1.7. Not let anyone remove equipment or records unless you are certain who they are;

8.1.8. Visitors and contractors in Trust buildings should always sign in a visitor's book.

8.2. Security of Paper Records

8.2.1. Paper documents should always be filed with care in the correct files and placed in the correct place in the storage facility.

8.2.2. Records that contain personal data, particularly if the information is sensitive should be locked away when not in use and should not be left open or on desks overnight or when you are not in the office;

8.2.3. Always keep track of files and who has them;

8.2.4. Do not leave files out where others may find them;

8.2.5. Where a file contains confidential or sensitive information, do not give it to someone else to look after.

8.3. Security of Electronic Data

8.3.1 Most of our data and information is collected, processed, stored, analyzed and reported electronically. It is essential that our systems, hardware, software and data files are kept secure from damage and unauthorised access. Trust staff must:

8.3.2 Prevent access to unauthorised people and to those who don't know how to use an item of software properly. It could result in loss of information;

8.3.3 Keep supplier's CDs containing software safe and locked away. Always label the CDs so you do not lose them in case they need to be re-loaded;

8.3.4 When we buy a license for software, it usually only covers a certain number of machines. Make sure that you do not exceed this number, as you will be breaking the terms of the contract.

8.3.5 Passwords are a critical element of electronic information security. All staff must manage their passwords in a responsible fashion:

8.3.6 Don't write it down;

8.3.7 Don't give anyone your password;

8.3.8 Your password should be at least 8 characters;

8.3.9 The essential rules your password is something that you can remember but not anything obvious (such as password) or anything that people could guess easily such as your name;

8.3.10 You can be held responsible for any malicious acts by anyone to whom you have given your password;

8.3.11 Include numbers as well as letters in the password;

8.3.12 Take care that no-one can see you type in your password;

8.3.13 Change your password regularly, and certainly when prompted.

Also change it if you think that someone may know what it is.

8.3.14 Many database systems, particularly those containing personal data should only allow a level of access appropriate to each staff member. The level may change over time.

8.4 Use of E-Mail and Internet

8.4.1 The use of the academy's e-mail system and wider Internet use is for the professional work of the academy. Reasonable personal use of the system in a member of staff's own time is permitted but professional standards of conduct and compliance with the Academy's wider policies are a requirement whenever the e-mail or Internet system is being used. The academy uses a filtered and monitored broadband service to protect our pupils. Deliberate attempts to access web sites that contain unlawful, pornographic, offensive or gambling content are strictly prohibited. Staff discovering such sites on the system must report this to their line manager immediately. The Principal will ensure that the sites are reported to the broadband provider for filtering.

8.4.2 To avoid a computer virus arriving over the Internet, do not open any flashing boxes or visit personal websites;

8.4.3 Do not send highly confidential or sensitive personal information via e-mail;

8.4.4 Save important e-mails straight away;

8.4.5 Unimportant e-mails should be deleted straight away;

8.4.6 Do not send information by e-mail, which breaches the Data Protection Act. Do not write anything in an e-mail which could be considered inaccurate or offensive, and cannot be substantiated.

8.5 Electronic Hardware

8.5.1 All hardware held within Academy should be included on the asset register;

8.5.2 When an item is replaced, the register should be updated with the new equipment removed or replaced;

8.5.3 Do not let anyone remove equipment unless you are sure that they are authorized to do so;

8.5.4 In non-secure areas, consider using clamps or other security

devices to secure laptops and other portable equipment to desktops.

8.6 Homeworking Guidance

8.6.1 If staff must work outside of the Trust or at home, all of the 'Information Security' policy principles still apply. However, working outside of the Trust presents increased risks for securing information. The following additional requirements apply:

8.6.2 Do not access confidential information when you are in a public place, such as a train and may be overlooked;

8.6.3 Do not have conversations about personal or confidential information on your mobile when in a public place. Ensure that, if urgent, you have your conversation in a separate room or away from other people;

8.6.4 If you use a laptop or tablet or smart phone

8.6.4.1 Ensure that it is locked and pass-word protected to prevent unauthorised access;

8.6.4.2 Make sure that you don't leave your device anywhere it could be stolen. Keep it with you at all times and secure it when you are in the Trust;

8.6.4.3 Any portable device or memory stick that contains personal data must be encrypted. Personal data may not be taking off the academy's site or put onto a portable devise without the express permission of the Principal. Taking personal data off-site on a devise or media that is not encrypted would be a disciplinary matter.

8.6.4.4 The Trust's Data Controller will maintain a register of: protected data that has been authorized for use on a portable devise; the fixed period of time that the authorisation relates to; the reason why it is necessary to place it on the device; the person who is responsible for the security of the device and its data; the nature of encryption software used on the device; confirmation of the date that the data is removed from the device.

8.6.5 When working on confidential documents at home do not leave them lying around where others may see them; dispose of documents using a shredder;

8.6.6 If you are using your own computer, ensure that others cannot access documents. When you have completed working on them, transfer them back to the Trust's system and delete them from your computer. It is forbidden to use a computer owned by you to hold personal data about pupils or staff at the Trust.

8.7 Audit of Data Access

8.7.1 Where possible our software specifications will include the function to audit access to confidential data and attribute access, including breaches of security, to specific users.

8.8 Data Backup

8.8.1 The Trust will arrange that all critical and personal data is backed up to secure on-line (off physical site) storage. If the academy is physically damaged critical data backups will allow the Trust to continue its business at another location with secure data.

8.8.2 Data backup should routinely be managed on a rolling daily process to secure off-site areas.

9 Disposal of Information

9.3 Paper records should be disposed of with care. If papers contain confidential or sensitive information shred them before disposing of them. Particular care must be taken when selecting papers to be placed in a recycling bin.

9.4 Computers and hardware to be disposed of must be completely 'cleaned' before disposal. It is not enough just to delete all the files.

9.5 It cannot be assumed that simply deleting a file will prevent it being recovered from electronic media. Electronic memory containing personal information or sensitive personal information must be electronically scrubbed or physically destroyed.

9.6 Where a third party contractor holds personal information on behalf of the academy, for example a payroll provider, the academy will seek reassurance from the contractor regarding their data protection policies and procedures.

10 Subject Access Requests

10.3 Requests from parents or pupils for access to personal data or educational records will be dealt with as described in the Privacy Notice for Parents and Pupils.

10.4 Trust staff may have access to their personal data within 30 calendar days of a request and at no charge.

10.5 Trust will maintain a documented record of all requests for personal information with details of who dealt with the request, what information was provided and when, and any outcomes. The record will be used if there is a subsequent complaint in relation to the request.

11 Sharing Personal Information

11.3 The academy only shares personal information with other organisations where there is a legal requirement to do so or the organisation has been contracted by the Trust to carry out a function of the academy.

11.4 The Trust is required, for example, to share information with the Department for Education and the Education Funding Agency. Under certain circumstances, such as child protection, we may also be required to share information with Children's Social Services or the police.

11.5 Because our pupils are of primary school age, their own right to access their own personal information held by the Trust will be exercised through their parents or guardians.

11.6 The Trust will be responsible for authorising the sharing of data with another organisation. The Trust, in authorising the sharing of data will take account of:

11.7 Whether it is lawful to share it;

11.8 Whether there is adequate security in place to protect the information while it is being transferred and then held by the other organisation;

11.9 Include in the Privacy Notice a simple explanation of who the information is being shared with and why.

11.10 Considerations regarding the method of transferring data should include:

11.11 If personal data is sent by e-mail then security will be threatened. You may need to check that the recipient's arrangements are secure enough before sending the message. The data may also need to be password protected and the password sent separately. You should also check that it is going to the correct e-mail address.

11.12 Circular e-mails sent to parents should be sent **bcc** (blind carbon copy) so that the e-mail addresses are not disclosed to everyone.

11.13 Similar considerations apply to the use of fax machines. Ensure that the recipient will be present to collect a fax when it is sent and that it will not be left unattended on their equipment.

11.14 If confidential personal data is provided by paper copy it is equally important to ensure that it reaches the intended recipient.

12 Websites

12.3 The Trust website will be used to provide important information for parents and pupils including our Privacy Notices and our Freedom of Information publication scheme.

12.4 Where personal information, including images, are placed on the web site the following principles will apply:

12.5 We will not disclose personal information (including photos) on a web site without the consent of the pupil, parent, member of staff or Governor as appropriate;

12.6 Comply with regulations regarding cookies and consent for their use;

12.7 Our website design specifications will take account of the principles of data protection.

13 CCTV

If the Trust uses CCTV this will be assessed using the Data Protection Impact Assessment process used for the purpose of assessing the privacy issues related to capturing images using CCTV which constitutes personal data. The Trust appreciates that images captured on CCTV constitute personal information under Data Protection regulations.

14 Photographs

14.3 The Trust may use photographs of pupils or staff taken for inclusion in the printed prospectus or other school publications without further specific consent being sought.

14.4 Images recorded by parents using their own personal equipment of their child in a school play or activity for their own family use are not covered by data protection law.

14.5 All other uses by the Trust of photographic images are subject to data protection regulations.

15 Processing by Others

The Trust remains responsible for the protection of data that is processed by another organisation (Data Processor) on its behalf. As part of a contract of engagement other organisations that process data on behalf of the Trust will have to specify how they will ensure compliance with data protection regulations.

16 Training

The Trust will ensure that all staff are adequately trained to understand their responsibilities in relation to this policy and procedures.

17 Freedom of Information Publication Scheme

In line with the Freedom of Information Act the Trust will provide its Approved Publication Scheme on our web site.

Information to be published	*How the information can be obtained*	*Cost*

Class 1 – Who we are and what we do

Who's who in the school	Prospectus and Website	Free
Who's who on the governing body and the basis of their appointment	Prospectus	Free
Instrument of Government	Prospectus	Free
Contact details for the Trust/Academies – telephone number and email address	Prospectus and Website	Free
School prospectus	From School Office/ e-mail/Website	Free
Staffing structure	Prospectus	Free

Class 2– What we spend and how we spend it

(Financial information relating to projected and actual income and expenditure, procurement, contracts and financial audit)

Annual budget plan and financial statements	Hard copy	Free
Capitalised funding	Hard copy	Free
Procurement and projects	Hard copy	Free
Pay policy	Hard copy	Free
Staffing and grading structure	Hard copy	Free

Class 3 – What our priorities are and how we are doing

(Strategies and plans, performance indicators, audits, inspections and reviews)

School profile Government supplied performance data The latest full Ofsted report	 Hard copy Hard copy	 Free Free
Performance management policy and procedures adopted by the governing body.	Prospectus	Free

Class 4 – How we make decisions

(Decision making processes and records of decisions) Current and previous three years as a minimum

Admissions policy/decisions (not individual admission decisions)	Prospectus	Free
Agendas of meetings of the governing body and (if held) its committees	Hard copy	10p/sheet
Minutes of meetings (as above) – n.b. this will exclude information that is properly regarded as private to the meetings.	Hard copy	10p/sheet

Class 5 – Our policies and procedures

(Current written protocols, policies and procedures for delivering our services and responsibilities). Current information only

School policies including: Charging and remissions policy Health and Safety Complaints procedure Staff conduct policy Discipline and grievance policies Single Equality Scheme	 Prospectus Hard copy Hard copy Hard copy Hard copy Hard copy	 Free Free Free Free Free Free

Home-school agreement Curriculum Sex education Special educational needs Accessibility Collective worship Pupil discipline	Website/Prospectus Website/Prospectus Website/Prospectus Website/Prospectus Website/Prospectus Website/Prospectus Website/Prospectus	Free Free Free Free Free Free Free Free
Records management and personal data policies, including: • Information security policies • Records retention destruction and archive policies • Data protection (including information sharing policies)	Website	Free

Class 6 – Lists and Registers

Currently maintained lists and registers only

Curriculum circulars and statutory instruments	Website/ Newsletters	Free
Any information the school is currently legally required to hold in publicly available registers **(THIS DOES NOT INCLUDE THE ATTENDANCE REGISTER)**	Hard copy	10p/sheet

Class 7 – The services we offer

(Information about the services we offer, including leaflets, guidance and newsletters produced for the public and businesses) Current information only

Extra-curricular activities	Website/Prospectus /Newsletters	Free
Out of school clubs	Website/prospectus /Newsletters	Free
Services for which the school is entitled to recover a fee, together with those fees	Hard copy	10p/sheet

Leaflets books and newsletters	Website/ School Office	Free
Additional Information *This will provide schools with the opportunity to publish information that is not itemised in the lists above*	None	

Contact details

Schedule of charges

This describes how the charges have been arrived at and should be published as part of the guide.

Type of charge	*Description*	*Basis of charge*
Disbursement cost	Photocopying/printing @ 10p per sheet (black & white)	Actual cost *
	Postage	Actual cost of Royal Mail standard 2nd class

* the actual cost incurred by the public authority