Information Security Policy

Approval Level:	Governing Body
Date Agreed:	Autumn Term 2020
Next Review:	Autumn Term 2021

Contents

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.

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.

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

REAch2 reserves the right to change this policy at any time.

2. Intended Impact

This policy is intended to ensure compliance with the GDPR and to give reassurance to anyone, who entrusts us with their personal data, that we take our responsibilities seriously and that we work to the highest standards to keep their data safe.

3. Roles and 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.

Any questions or concerns about your obligations under this policy should be referred to your line manager, the HR Team, or the Data Protection Officer (DPO). Questions and concerns about technical support, or for assistance with using the Trust's IT systems, should be referred to it@reach2.org in the first instance.

4. National Guidance and Statutory Requirements

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).

5. Critical School Personal Data

Data protection is about protecting information about individuals. Even something as simple as a person's name or their hobbies can count as Personal Data.

Some Personal Data is very sensitive, which was formerly categorised as 'sensitive personal data and has been renamed by the ICO as 'special category' data. In REAch2 policies, this is called Critical School Personal Data. It includes information on:

- Child protection matters;
- Serious or confidential medical conditions
- Special educational needs;
- Financial information (for example about parents and staff);
- Racial or ethnic origin;
- Political opinions;
- Religious beliefs or beliefs of a similar nature;
- Trade union membership;
- Health (including physical or mental health and covers the provision of health care services)
- Genetic information;
- Biometric information;
- Sex life;
- Sexual orientation.

This following is treated as would have been sensitive personal data but is broader and linked to security measures:

- criminal offence (including criminal convictions and offences or related security measures). Note: includes 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).

6. Minimising the Personal Data Held

Restricting the amount of personal data we hold to that which is needed helps us to keep personal data safe. The REAch2 Information and Records Retention Policy provides guidance on when to delete certain types of information. If you are unsure, speak to your line manager, Safeguarding Lead, HR or the DPO.

7. Privacy on a Day to Day Basis

We should be thinking about data protection and privacy whenever we are handling Personal Data.

From May 2018, the Trust is required to carry out an assessment of the privacy implications of using Personal Data in certain ways. For example, when we introduce new technology, where the processing results in a risk to an individual's privacy or where Personal Data is used on a large scale, such as closed-circuit television (CCTV).

These assessments help the Trust to identify the measures needed to prevent information security breaches from taking place.

8. Using Computers and IT

Data protection breaches can happen as a result of basic mistakes being made when using the Trust's IT system. Below is guidance on keeping information secure:

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 lock your screen, please speak to IT.

Be familiar with the Trust's IT
Make sure that you familiarise yourself with any software or hardware that you use - in particular that you understand what the software is to be used for and any risks. For example: if you use a 'virtual classroom' which allows you to upload lesson plans and test papers for pupils then you need to be careful that you do not accidently upload anything more confidential.

Make sure that you know how to use any security features contained in Trust software. For example, some software allows you to redact documents (i.e. 'black out' text so that it cannot be read by the recipient). Make sure that you can use this software correctly so that the recipient of the document cannot 'undo' the redactions.

You need to be extra careful where you store information containing Critical School Personal Data. If safeguarding information is saved on a shared computer, access should be limited.

If in doubt, speak to the IT Team for specific guidance on the information security arrangements of the different programmes that the Trust uses.

Hardware and software not provided by the Trust
No software, application, programme, or service should be downloaded without permission from the Head of IT. All queries relating to the installation of software should be directed to the IT Support Portal.

Staff must not connect (whether physically or by using another method such as Wi-Fi or Bluetooth) any personal device or hardware to the Trust IT systems without permission.

Private cloud storage

You must not use private cloud storage or file sharing accounts to store or share Trust documents.

Portable media devices

The use of portable media devices, such as USB drives and portable hard drives is not allowed unless those devices have been given to you by the Trust and you understand how to use those devices securely. Any equipment provided by the IT Department will be protected with encryption software. All USB drives provided by an academy should be encrypted.

Disposal of Trust IT equipment

Trust IT equipment, including laptops, printers, phones, and DVDs, must always be returned to the IT Department even if you think that it is broken and will no longer work.

Passwords

Passwords should be difficult to guess. Do not use information which other people might know, or be able to find out, such as your birthday or your partner's name.

Do not write down your password.

Your password should not be disclosed to anyone else.

You must not use a password which is used for another account. For example, you must not use your password for anything private for a school account.

Passwords, along with any other security credentials issued to you such as a key fob or USB drive, must be kept secure and not be shared with anyone else.

Emails

When sending emails or faxes, take care to make sure that the recipients are correct. Use BCC when sending an email message to multiple recipients so you don't share everyone's email address – or ask permission.

Private email addresses

You must not use a private email address for Trust related work. Use only your school or REAch2 email address. This applies to Governors as well. Please speak to the IT Department if you require an email account to be set up for you.

Encryption
Remember to encrypt internal and external emails which contain Critical School Personal Data. For example, encryption should be used when sending details of a safeguarding incident to social services. If you need to give someone the password to unlock an encrypted email or document, this should be provided via a different means and not included in the same email.

9. Paper Files

Put papers away
Keep a tidy desk and put papers away when they are no longer needed.

Keep under lock and key
Papers which contain Personal Data should be kept under lock and key in a secure location and not left unattended on desks, unless the room is secure. Any keys must be kept safe.

If papers contain Critical Personal Data they must be kept in secure cabinets identified for the specified purpose. For each cabinet, set out who has access, and who has the key. There should be at least two people so it can always be accessed in an emergency.

Information must not be stored in multiple locations, unless absolutely necessary, for example, child protection information should be stored in only one location in a secure cabinet.

Disposal
Paper records containing Personal Data should be disposed of securely by placing them in confidential waste bins. Personal Data should never be placed in the general waste.

Printing
When printing documents, make sure that you collect everything from the printer straight away, otherwise there is a risk that confidential information might be read or picked up by someone else. If you see anything left by the printer which contains Personal Data, you must hand it in to your line manager. If possible, use 'follow me' printing which means that you cannot print something out unless standing by the printer.

Post
Confidential materials should be sent registered post to ensure it is received only by the person intended.

10. Working Off Site

Staff might need to take Personal Data off the school site for various reasons, for example because they are working from home or supervising a school trip. This does not breach data protection law if the appropriate safeguards are in place to protect the Data.

For school trips, the trip organiser should decide what information needs to be taken and who will be responsible for looking after it. Personal Data taken off site should always be returned to the school.

Anyone working from home should check with IT what additional arrangements are in place. This might involve installing software on a home computer or smartphone.

Take the minimum with you
When working away from the school, take the least amount of information with you.

Working on the move
You must not work on documents containing Personal Data whilst travelling if there is a risk of an unauthorised disclosure, for example if you are in a public place where others may see the laptop screen. Do not leave any device unattended.

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

- kept in a locked case or secure in your possession at all times;
- out of plain sight in a car. Possessions left on car seats are vulnerable to theft when your car is stopped e.g. at traffic lights.

If you have a choice between leaving documents in a vehicle and taking them with you, then you should take them with you. If you have to leave paperwork in a car, make sure it is out of sight.

Public Wi-Fi
Do not use public Wi-Fi to connect to the internet if you are working on sensitive data. If you are unsure, you should work offline until you can connect to a secure WiFi. Only devices issued by the Trust should be used as personal hot spot.

Using Trust laptops, phones, cameras and other devices
If you need the use of a Trust device, then speak with your line manager.

Critical Personal Data should not be taken off the site in paper format except for specified situations where this is absolutely necessary and the information is not available in another, more secure, format.

11. Using Personal Devices for Trust Work

Using your own PC or Laptop
If you use your laptop or PC for Trust work you must use Cloud based software.

The Trust is progressing a programme of work to facilitate this for all academies.

Using approved software means that Personal Data is accessed through the Trust's own network which is more secure and significantly reduces the risk of a security breach.

Using your own smartphone or handheld device
The use of personal smartphones or handheld devices for work is not encouraged. If you must use a personal device, you should install the management software provided by the Trust which will help to keep Personal Data secure.

This software has a remote wipe functionality which can be invoked should the device be lost or stolen. The Trust reserves the right to monitor, review and erase, without further notice, all content on the device that has been created for the Trust or on the Trust's behalf or which contains Personal Data. Although we do not intend to wipe other data that is private, such as photographs, private files or emails, it may not be possible to distinguish all such information from Trust Data in all circumstances. You should therefore regularly back up any private data.

You must not do anything which could prevent any software installed on your computer or device by the Trust from working properly. You must not try and uninstall the software or save Trust documents to an area of your device not protected, without permission from the IT Department.

Appropriate security measures should always be taken. This includes the use of firewalls and antivirus software. Any software or operating system on the device should be kept up to date.

Default passwords
If you use a personal device for schoolwork which came with a default password this password should be changed immediately. This policy provides guidance on choosing a strong password.

Sending or saving documents to your personal devices

Documents containing Personal Data, including photographs and videos, should not normally be sent to or saved to personal devices unless you have been given permission by the IT Department. This is because anything you save to your personal computer; tablet or mobile phone will not be protected by the Trust's security systems.

Friends and family

Take steps to ensure that others who use your device cannot access anything related to your work. You must not share login details with others, and you should log out of your account once you have finished working by restarting your device.

When you stop using your device for Trust work, for example:

- if you decide that you do not wish to use your device for Trust work;
- if the Trust withdraws permission for you to use your device;
- if you are about to leave the Trust

then, all Trust documents, including emails, and any software applications provided for Trust purposes, will be removed from the device.

If this cannot be achieved remotely, you must submit the device to the IT Department for wiping and software removal. You must provide all necessary co-operation and assistance to the IT department in relation to this process.

12. Data Breach

Information security breaches can happen in a number of different ways, for example:

- an unencrypted laptop is left on a train;
- a mobile phone is stolen;
- a website is hacked;
- a confidential email is sent to the wrong recipient.

Any security incidents, breaches and weaknesses should be reported immediately to your line manager, HR or the DPO. This includes anything you become aware of even if you are not directly involved, for example you discover a document storage room unlocked or confidential information left out on a desk overnight.

In certain situations, the Trust must report an information security breach to the Information Commissioner's Office (ICO), 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 you report breaches immediately.

13. Breach of this Policy

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

A member of staff who deliberately or recklessly discloses Personal Data held by the Trust without proper authority may also be guilty of a criminal offence and gross misconduct. This could result in summary dismissal.