five communities + one vision

Ratton School
achieving together

RATTON SCHOOL

AN ACADEMY TRUST
SPECIALISING IN THE PERFORMING ARTS

DATA PROTECTION POLICY

Date approved by governors	July 2017
Date of next review	July 2018
Status	Statutory

All our policies support our <u>vision</u> and are based on our <u>core virtues</u>

Developing caring, confident and creative students who achieve excellence

- **Compassion**
- **Respect**
- **Creativity**
- **Teamwork**
- **Effort**
- **Responsibility**

1. Introduction

All members of Ratton School Academy Trust have a personal responsibility to ensure that they follow the requirements of legislation relating to information security contained in the following Acts.

- Data Protection Act 1998
- Computer Misuse Act 1990
- Freedom of Information Act 2000
- Human Rights Act 2000.

What is Personal Information?

Personal information or data is defined as data which relates to a living individual who can be identified from that data, or other information held.

Members of the Academy are expected to take all reasonable steps to protect data and not take risks that expose the Academy to breaches of the above Acts, by using the guidance contained within this policy.

All data losses are serious, but where large numbers of people are affected (over 1,000 individuals), the impact is much greater, as are the consequences. The Academy needs therefore to apply high levels of data protection because of its role in providing a wide range of educational and welfare services.

Staff handling sensitive and confidential data must assume personal responsibility and make considered judgements in terms of how they handle data.

Student members of the Academy need to safeguard their data to ensure they stay safe and protect their intellectual property. Students will be taught in lessons how to minimise on-line risks and what to do in cases of cyber-bullying.

The Academy will monitor the use of data to: prevent and investigate breaches of the policy and detect data misuse; reduce repair costs resulting from criminal damage; apprehend and if necessary prosecute offenders; reduce insurance costs; monitor security of premises and vehicles; provide greater personal protection for staff, students and members of the public. [The monitoring will be by electronic and CCTV systems.]

Serious breaches of data protection or computer misuse could result in disciplinary or legal action being taken against individuals of the Academy.

The Academy will authorise specific personnel to be responsible for data protection and safeguarding, nominate and appoint a Senior Assistant Headteacher.

2. Purpose of this Policy

This document is intended to:

- prevent unauthorised disclosure of information by laying down clear standards of practice to maintain good security
- procedures that should be followed to safeguard and protect young people
- to clarify how data could be used for pursuing criminal activities and how data information could be obtained under the Freedom of Information Act.

3. Scope and who the policy applies to:

The scope covers all circumstances where sensitive or confidential data of the Academy are stored or taken outside of their normally secure location. This includes data in all formats – non-electronic (paper) and electronic forms.

The Policy will still apply outside of the school premises when Academy data is contained or downloaded onto devices or connected over a Virtual Private Network, or via the internet to the school network (Local Area Network). For example when data is transferred to:

- Personal home computers
- Personal laptops and tablets
- Removable storage media
- Mobile phone technology.

The Policy applies to employees and student members, temporary staff, volunteers, and other agencies that may use Academy data.

4. Responsibilities

Ratton School Academy Trust maintains appropriate security and privacy of data that it uses to perform its functions and it will ensure that appropriate tools, training and guidance are available to staff, student members and others who may require access to digital resources and data.

The Academy will take steps to provide a:

- Secure network for storing and using electronic data whether held internally or cloud based
- Secure work locations for storing and using hard-copy data
- Encryption tools for transmission of data outside the secure locations when appropriate to the risks involved.

Academy staff will act in accordance with the following standards and guidance to ensure security and privacy of sensitive and confidential data outside of their normally secure location.

Service delivery partners and agencies that use Academy data for our service delivery will have to confirm they comply with these or equivalent standards.

Where secure data-sharing protocols are required for example, with multi-agency data sharing, the Academy will take appropriate actions to meet the security standards specified in such agreements. In all other respects the Academy and its members must work to the standards set out in this policy.

5. Disciplinary and other Sanctions

Where Academy employees or service delivery partners have acted in accordance with this standard, but a breach occurs through the action of others, they will be deemed to have acted reasonably.

If Academy employees and members are found to be in breach of the policy and its guidance then they may be subject to disciplinary procedures.

GUIDANCE FOR STAFF, TEMPORARY STAFF, AND VOLUNTEERS

Working with electronic files and data:

Electronic files should be saved to the network server systems to the appropriate area and decisions made if the document needs to have restricted access, and if restricted access is required at what level.

Files and records that are copied onto memory sticks (USB devices), and external hard drives should be only taken off-site for home-working and should not contain personal or financial information that could be damaging for the Academy if lost or should fall into criminal hands.

Personal laptops and mobile technology should be password protected and closed down from the system when left unattended.

Basic precautions when using mobile technology:

- Take all reasonable steps to keep the device and data safe and secure
- Keep it with you whenever possible; lock it away securely when you can't
- Never leave it in plain sight in public places
- Never let others use your access or device
- Delete all unnecessary data from the device as soon as possible
- Keep the password securely and separately from the device
- Report loss/theft immediately to the Academy's Senior Assistant Headteacher.

Only authorised and monitored e-mail services should be used on Academy network equipment. Web-based public access e-mail systems should not be used.

Before sending or taking sensitive or confidential data outside of the Ratton School Academy Trust premises, staff should make the following checks and consider:

- If you are sending more detail than is necessary?
- Is the data you are sending correct and appropriate for the task?
- If you are sending the data to the correct person and address?
- How you intend to keep it secure in the external location?
- Should you be using an authorised secure data transfer system?

Home-working with a personal computer, laptop and mobile devices

If you are working at home on your own personal computer or laptop you must:

- Only work on sensitive or confidential data that you can access via the Virtual Private Network (Microsoft Remote Desktop and Foldr) gateway when using programmes such as the School Information Management system (SIMs). You must not transfer sensitive or confidential data onto your home PC or laptop
- Only have as much sensitive or confidential information open as necessary and only for as long as necessary
- Always save the data back to the normally secure location when you have finished
- Not leave the computer unattended for any period of time such that others can access any sensitive data; always lock the computer or log out when you are not using it

Using the Web Portal (Microsoft Remote Desktop and Foldr)

If you are transferring sensitive or confidential data through a web portal (Microsoft Remote Desktop and Foldr) to an external device you must:

- Ensure that there is robust access control in place (i.e. unique username/password) on the external device
- Ensure that only the people who need the data can see it
- Delete the data from the device as soon as possible.

Sending e-mails using MS Outlook Exchange

- Make sure the recipient is known and trustworthy
- Make sure the electronic message is traceable (apply delivery and read receipts) when considered appropriate.

Mobile Storage Devices

If you carry data with you on a mobile storage device, such as a tablet PC, laptop, USB memory stick, or a mobile phone you must:

- Make sure that there is no other more secure option available to you
- Take only as much as necessary, for as long as necessary and transfer them back to their normally secure location as soon as possible
- Keep passwords securely and separately from the device data preferably memorised
- Take all reasonable precautions to keep the device and data safe and secure by whenever possible by locking it away securely
- Never leave it in plain sight in public places
- Never let others use your access or device
- Delete the data from the device as soon as possible
- Report any loss / theft immediately to the Trust's authorised Information Asset Manager.

Using Approved Secure Transfer of Data Mechanisms

The Academy uses a range of approved and secure transfer mechanisms that should be used for commercially sensitive and confidential purposes. Examples of this are:

- ESCC Secure Email
- AVCO (software that allows secure transfer of documents)
- School to School (S2S)
- Government Connect (GCSX).

Using Fax equipment

Sending sensitive or confidential information by fax is a last resort and should only be used if the need is urgent and there is no alternative available and you must:

- Make sure the receiving fax machine is in a secure environment
- Make sure the recipient is there to receive it at the time of arrival and that they are known and trusted
- Make sure it is traceable (e.g. confirmation of receipt).

Using Postal services

The postal service is considered reasonably secure for small amounts or low impact data (i.e. records pertaining to an individual, but NOT including very sensitive personal data – Data Protection Act). There are precautions that you must take to prevent loss:

- Make sure that the recipient and destination address is correct, accurate and up-to-date
- Clearly mark the envelope or parcel with a return address in case of incorrect delivery
- Do not send the only copy of the data if it is practical to make and retain a duplicate. You must assess the impact of loss of the original and make a copy if that impact is unacceptable
- If you use a courier they must be known and trusted
- Make sure it is traceable (i.e. confirmation of receipt)
- Physical records must be sent in a suitable container that is robust and secure enough to prevent accidental loss or tampering.

Using Physical (Paper) Records

If you are taking sensitive or confidential information with you in non-electronic (paper) records you must:

- Make sure that there is no other option available to you
- Never take the only copy with you if it is practical to make and retain a duplicate.
- You must assess the impact of loss of the original and make a copy if that impact is unacceptable
- Take only as much as necessary and only for as long as necessary
- Transfer it back to its normally secure location as soon as possible
- Take all reasonable precautions to keep the records safe and secure

How to avoid unnecessary data loss risks by not:

- Storing sensitive or confidential data on any personal equipment or in an unencrypted form.
- Sending sensitive or confidential information as unsecured physical records
- Working on sensitive or confidential data on a public personal computer or laptop (for example in a library or cafe)
- Working on sensitive or confidential data on a personal computer or laptop with an unencrypted wireless (WiFi) connection. There is a requirement to ensure your home wireless network has encryption and is switched on
- Leaving sensitive or confidential physical records in plain view of others or where they can be overlooked by others
- Leaving any device holding sensitive or confidential information unattended in plain view of others.

What to do if data loss occurs:

In the first instance staff should report a loss of sensitive or confidential data to their line manager. The line manager should then report the loss to the Senior Assistant Headteacher, detailing the circumstances of the loss and the nature of the data lost. The Senior Assistant Headteacher can then advise and take the appropriate action.

Requirements of the Freedom of information and Data Protection Acts that affect Ratton School Academy Trust

The **Freedom of Information** Act requires the Ratton School Academy Trust to release information to anyone requesting it.
The **Data Protection Act** contains eight principles for processing (using) personal information.
All Personal information must:

1. Be fairly and lawfully processed
2. Be processed for limited purposes
3. Be adequate, relevant and not excessive
4. Be accurate and up to date
5. Not be kept longer than necessary
6. Be processed in line with the data subjects' rights
7. Be secure,
8. Not be transferred to other users without adequate protection.

It covers:

- All data relating to a living individual.
- Any data classified as Commercial in Confidence – e.g. data that relates to commercial proposals or current negotiations
- Any data relating to investigations and proceedings, information provided in confidence etc.