Fulston Manor Academies Trust

Data Protection Policy

(Including Cyber Security)

Fulston Manor School

South Avenue Primary School

Version (Date):	**July 2023**
Review (Date):	**July 2024**
Member of Staff Responsible:	**Mrs M Smith**

1. Data Protection Context.
Fulston Manor Academies Trust (the Trust) is registered as a single entity with Companies House Reg no 07343725. As such it provides governance and oversight for compliance with Data Protection Act and the EU General Data Protection Regulation (GDPR). This applies to all schools forming part of the trust including Fulston Manor School and South Avenue Primary School. This policy provides information to; our pupils, their parents and guardians, staff, governors, customers, and any other third party who may use our services, engage with our establishment, or act as a supplier on how we go about protecting their privacy and freedoms.

The Data Protection Act 2018 including the General Data Protection Regulations (GDPR) promote high standards in the handling of personal information including the protection of individuals' rights to privacy. It applies to all organisations processing information about living individuals using digital and paper records. Data Controllers must follow the six data principles of data protection and other aspects of the legislation. These say that personal information must be:

- Be processed lawfully, fairly and transparently
- Used for a specific, explicit & legitimate purpose with no incompatible processing
- Adequate, relevant and not excessive
- Accurate and kept up to date and rectified or erased if inaccurate
- Not kept for longer than is necessary
- Processed securely

Also:

- The rights of data subjects are fully embraced
- The responsibilities of data controllers and data processers are understood and followed
- That the transfer of personal data beyond the EEA is done securely and lawfully

2. Data Controller Registration.
The trust is registered as a Data Controller with the Information Commissioners Office - reference no. ZA801991. We process personal data for the purpose of providing education, training, welfare and educational support services, to maintain school property; maintain accounts and records, undertake fundraising; and to support and manage our employees. We also use CCTV at some of our schools for security and the prevention of crime.

3. Organisational Structure.
The trust is a multi-academy trust formed of the following schools:

Fulston Manor School
South Avenue Primary School

As a trust, the Articles of Association determine our Governance Structure. The trust is overseen by members and trustees, whose details are published upon our websites www.fmat.org, www.fulstonmanor.kent.sch.uk and www.southavenue.kent.sch.uk.

The role of the members is to ensure compliance with the Articles of Association. The trustees/governors provide a strategic layer of governance across the entire trust. Each trustee has a themed responsibility, the Chair of the Trust Board has overall responsibility for Information Management, including our compliance with the Data Protection Act and the Freedom of Information Act.

The Headteacher/Head of School or their nominees are responsible for the day to day running of their school, this responsibility includes collecting and processing personal data for educational purposes relative to their school. In respect to the governance arrangements required for information management, they perform the role of Information Asset Owner (IAO).

The Executive Headteacher performs the role of SIRO, this responsibility includes providing guidance to Information Asset Owners (IAO), identifying Information Asset Owners for all assets and ensuring they understand responsibilities and having oversight of and prioritisation of Information Governance activities.

Key legislation relevant to this policy include:

Data Protection Act 2018 including the General Data Protection Regulations. (GDPR)
The Freedom of Information Act 2000
The Education (Pupil Information) (England) Regulations 2005
The Education Act 1996

4. Lawful Basis for Processing.

The personal data processed by the trust is wide ranging. We collect and process data under the following lawful basis: Legal Obligation, Consent and Public Interest. The data predominantly relates to Pupils, Parents and Guardians, Teachers, Staff, Contractors, Volunteers, and other persons with a formal or informal relationship with any of the schools in the trust group.

We are required by law, to provide information about our pupils to the DfE as part of a national requirement for the collection and processing of personal data, including completion of the school census and early years' census. Some of this information is then stored in the National Schools Data Base (NPD). The law that allows this in the Education (Information About Individual Pupils) (England) Regulations 2013.

There may be circumstances where it is necessary to use personal data to support other school activities not specifically included in the legislation referred to above. Examples may include setting up communication links between pupils, parents and a school, the use of other information such as photographs of pupils to appear in newsletters, on our web site, social media or in the newspaper media. In these circumstances we seek written consent from the parent or guardian, which we review with annually. A privacy notice has been published on our website providing a transparent explanation of out processing.

5. Complementary Policies

This policy provides overarching governance for data protection, we have other policies that complement it, and offer more detailed guidance in more specialist topics. These should be read in conjunction with this policy and can all be found on our website under the "Info" Tab.

6. Information Assets

Personal data is recorded in automated (digital) and manual formats, also digital images are captured on CCTV systems; these are covered by separate policies which are reviewed annually and can be found on our website.

7. Policy and its Purpose

The aim of this policy is to define the manner and purpose as to how personal data is used, including, its collection, recording, organisation, structuring or storage, adaption, alteration, retrieval, dissemination, restriction, security, erasure or destruction of data is carried out.

The intention of this data protection policy is to:

- Ensure the trust is compliant with data protection law and follows good practice.
- Safeguards the privacy and rights of pupils, parents and guardians, teachers and staff, contractors, volunteers and other data subjects
- Mitigate against potential threats posed by cyber criminals
- Encourages openness in how it collects, manages, and disposes of individual's data.
- Ensures data is processed securely and to avoid the risk of inadvertent breaches
- Provides governance and guidance for staff, contractors and volunteers

8. Scope.
This policy is applicable to:

- All of the schools forming part of the trust including the pupils, parents and guardians, teachers and staff, contractors, volunteers and those working in it or visiting it on a temporary basis
- All pupils, parents or guardians, teachers and staff, contractors and volunteers when involved in activities outside of the main premises belonging to the trust including attending off site events or working from home, otherwise called remote working
- Contractors, suppliers and other people working for or acting on behalf of the trust

It applies to all personal data processed by the trust relating to identifiable individuals when delivering education, even if that information technically falls outside of the Data Protection Act 2018 and GDPR. This includes:

- Names of individuals
- Physical and Mental Ailments
- Religious Beliefs
- IP Addresses
- Postal addresses
- Email addresses
- Biometrics
- Telephone numbers
- Digital images
- Plus, any other information relating to individuals.

9. Responsibilities.
Every member of staff, contractor or volunteer are required to read and comply with the contents of this policy.
Everyone who directly handles personal data must ensure they do so in accordance with this policy and data protection principles.

The members and trustees are responsible for ensuring the trust meets its legal obligations.

The Leadership Group is responsible for:

- Directing the manner and purpose for how personal data is used and transparency in how it is processed
- Keeping the members & trustees updated about data protection responsibilities, risks and issues
- Reviewing technical countermeasures and policy compliance, in line with an agreed audit schedule
- Arranging data protection training and advice for the people covered in this policy

- Responding to data protection questions from staff and anyone else mentioned in this policy
- Managing requests from individuals to see the data the trust holds about them (Subject Access Requests)
- Checking and approving any contracts and agreements with third parties that may process, handle or access personal data on behalf of the trust
- Approving any data protection statements attached to letters and emails
- Addressing data protection queries from external bodies such as the media
- Working with other members of staff to ensure any promotional initiatives comply with data protection principles

The IT used by the trust includes the use of national and locally provided databases and systems. Out IT systems are maintained by our in-house IT Support Technicians who ensure all systems, services and equipment used for storing data meet acceptable security standards.

- Perform regular security checks to ensure security hardware and software is functioning correctly
- Evaluating any third-party services the trust is considering using for the storage or processing of its data
- Taking immediate action to respond to any suspected or actual Cyber Security threat
- Maintain an up to date asset registers for physical (hardware) as well as information assets

Access to personal data, is determined by the role and functional responsibilities of teaching staff, support staff, volunteers and those with either management or administrative positions. Personal data can only be accessed or used for a specific, explicit and legitimate purpose as set out earlier in this policy. It should not be assumed that personal data processed lawfully by the trust is automatically available to everybody working in it.

10. General Staff Guidance.

Every member of staff is provided with data protection training, training records are maintained by the HR Team. Likewise, staff are expected to read and acknowledge their understanding of the contents of this policy.

The personal data held is not shared informally. Access to sensitive information is controlled.

Access to the various databases used by the trust is tiered, requiring separate passwords to provide controlled access relative to their role.

The trust provides guidance and advice to help staff understand their responsibilities and keep those skills up to date to reduce the risk of inappropriate loss of personal information.

Teachers, Staff, and volunteers take appropriate precautions to keep all data secure by following the guidance contained in this policy.

The trust has a password policy to ensure that strong passwords are used, not shared, and changed frequently. Passwords should comply with the rules as laid out in the IT Policy – Acceptable Use Policy.

Teachers, Staff, Contractors, and Volunteers understand that personal data must not be disclosed to unauthorised persons, either within the trust or to anybody external to it.

Personal data is regularly reviewed and updated by the HR department. Only that which is adequate,

relevant and not excessive in relation to providing education is processed and not retained unless it is necessary.

Teachers, Staff, Contractors, and Volunteers should seek advice and guidance from either the Headteacher/Head of School, or a member of the Leadership Group if they are unsure about any aspect of data protection.

Cyber- crime represents a serious threat to the efficient operation of our school. Specific guidance for staff is outlined in Appendix A.

11. IT Acceptable Use Including Remote Working.
Remote or offsite working offers flexibility and benefits for staff as well as the trust. It also carries additional risks to information security. To mitigate such risks we have in place a specific policy titled ICT Acceptable Use Policy for Staff, part of the trust IT Policy -which can be found on our website.

It is a condition of this policy, that staff are not permitted to carry out any remote working unless they have read, understood and are able to comply with the contents of the ICT Acceptable Use for staff Policy.

12. Data Use.
When working with personal data staff are instructed to make use of screensavers and to lock them when unattended, also to ensure their screens cannot be viewed or accessed by unauthorised persons when in use.

Strict access protocols are used to ensure only trained staff are granted access to automated and manually stored personal data, access is only granted when relevant to work performed in specific roles.

Staff are encouraged to exercise great care when using email, or conventional postal services to prevent personal data being unlawfully disclosed, misdirected or lost.

Personal data is never transferred outside of the European Economic Area.

Teachers, Staff, Contractors, and Volunteers are not permitted to save or use personal data controlled by the trust on their own personal computer, smart phone, laptop or tablet unless authorised in advance by the trust, and used in strict compliance with this policy.

13. Data Accuracy.
All Teachers, Staff, Contractors, and Volunteers understand that it's a legal requirement for the personal data they collect and process to be accurate and kept up to date.

The more sensitive or important the personal data is, additional effort is made to safeguard its security.

The type of personal data processed by the trust is minimised and stored in as few places as possible, Teachers, Staff, Contractors, and Volunteers are encouraged not to create duplicate or additional data sets, such as mailing lists or bespoke spreadsheets.

Teachers, Staff, Contractors, and Volunteers take every opportunity to test the accuracy of the data held by the trust e.g. validating personal information with pupils and parents during routine communication.

Each school uses a generic web site, each has local autonomy to update its contents independently. This is to enable pupils, parents and members of the public up to be provided with useful

information and updates on matters of interest. The websites enable pupils and parents to complete applications for various school functions. They do use cookies; the cookies policy is accessible on each website.

Personal data is updated as soon as inaccuracies are discovered e.g. prompted when email addresses generate a message delivery failure response, or telephone numbers listed cannot be reached.

Data is retained no longer than is necessary. As regards South Avenue Primary School, in most cases personal data relating to pupils is passed on to their new school (which may be Fulston) and removed from their own systems. We have a retention policy which sets out in more detail how long we retain the various types of records we deem it is necessary for us to retain.

It is the responsibility of each individual school secretary or dedicated administrator to ensure that records are kept no longer than is required by referring to our records retention schedule. If in exceptional circumstances it is necessary for certain records to be retained longer than defined in our schedule, a record is made of the decision, and that decision is reviewed periodically.

14. Technical and Physical Security.

It is everybody's responsibility to maintain vigilance during normal business hours, this includes verifying the identity of visitors, checking that only persons who our authorised are admitted, visitors are supervised, and access to any parts of the trust's premises containing sensitive information is controlled.

The security of our premises is maintained to a high standard. CCTV is employed at both of our schools for the prevention of crime and to ensure the safety of pupils and staff. The Information Commissioners codes of practice are used to assess and justify their use. Strict access controls are in place to limit the members of staff with permission to view, access or download images from the systems.

Site access at both schools is controlled using a common policy permitting access to only those whose identification has been verified and who need to be physically present. Access permission will be limited to only those parts of a building where it is necessary for access and or to perform a specific task.

Technical measures are in place to protect the personal data stored electronically to protect it from unauthorised access, accidental deletion and vulnerability to cyber- attacks. This protection is reviewed by the Network Manager annually.

If personal data is stored on removable media, such as CD, DVD or memory sticks, these are encrypted or where this is not technically feasible then alternative safeguards are employed to mitigate against the risk of accidental or unlawful loss or use of personal data.

Data relating to children in our care and staff is stored on designated servers and drives on internal secure storage.

Servers or files containing personal data relating to children and staff are annexed from those used for general administration.

Secure back- up systems are used to protect the personal data processed by the trust.

Personal data controlled and processed by the trust is not permitted to be saved directly to laptops or other mobile devices such as smart phones or tablets, other than those authorised for use by the

trust.

The use of smart phones and tablets belonging to pupils, parents, and staff whilst in our schools is governed by a specific Mobile Phone Policy and Acceptable use Policy contained within the trust IT Policy. Compliance with its contents is a requirement of this policy.

Manual records, such as paper records and files, including documents printed from digital records, are kept in a secure place where unauthorised people cannot access, view or copy them. They are not to be removed from school premises unless with the explicit consent of the nominated information asset owner (IAO) or head teacher.

15. Disposal of Data, Hardware & Documents.

All staff and volunteers who leave the trust are required to hand over all hardware issued to them by the trust, and delete any personal data and return any documents containing personal data they accessed and used during their tenure. Their access rights to any of the systems used by the trust, including the contents of any data base or manual filing system under the control of the trust will be removed as soon as practicable following their leaving date. Under no circumstances can they retain any personal data including images unless it is with explicit consent of the Headteacher/Head of School acting in the capacity of data controller.

When disposing of old computer hardware or removable media, extreme care is exercised to ensure that all personal data is wiped from its memory. The disposal is overseen by the Network Manager, the operation to cleanse personal data from a computer or device is recorded.

A record retention schedule specific to education is used to ensure data storage limitation is adhered to. Each school has an appointed member of staff responsible for managing records.

Similarly, great care is exercised when storing and destroying paper documents which contain personal data. These types of records are destroyed securely by a third party or shredded on site by school secretaries. Records are maintained of how when and where such records were destroyed.

16. Data Breaches.

A data breach is defined as a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure or access to personal data transmitted, stored or otherwise processed.

All Staff, Contractors, and Volunteers have a responsibility to escalate any potential security risks, or actual breaches as defined above to their line manager immediately.

Any breach or “near miss” should also be escalated immediately to the Headteacher/Head of School who is responsible for notifying the Data Protection Officer (DPO). The DPO will investigate the incident and assess whether or not it meets the ICO reporting criteria. The DPO will liaise with the Headteacher/Head of School or their nominee and assess all available information. If the circumstances meet the ICO reporting criteria, the DPO is responsible for notifying the Information Commissioners Office of the breach within 72 hours of it becoming known. Assistance will be provided by the contracted DPO who will assist the investigation management of the breach including working with the regulator.

Where a breach could seriously affect the psychological or the physical well-being of an individual, or individuals, the Headteacher/Head of School or their nominee must take immediate steps to contain the breach and notify the individual(s) concerned that a breach has occurred.

A record of breaches, near misses, Subject Access Requests, and Freedom of Information Requests is maintained on behalf of the trust, including information as to how any lessons learned have been disseminated to Teachers, Staff, Contractors, and Volunteers and or contractors.

17. Continuous Improvement

The trust encourages Teachers, Staff, Contractors, and Volunteer staff to be mindful of the need to safeguard the privacy of our pupils, parents and guardians, teachers, staff, volunteers and contractors personal data.

Teachers, Staff, Contractors, and Volunteers are provided with guidance and encouraged to report actual or potential security breaches.

In addition:

A data protection compliance audit is carried out at each school annually by the DPO, records are made of each audit and maintained on behalf of the trust.

Teachers, Staff, Contractors, and Volunteers are provided with threat and risk awareness guidance relative to their role.

Guidance promoting information security is on display in appropriate parts of our premises.

18. Data Subject Rights.

The trust understands the rights of those whose personal data we process and will facilitate those wishing to exercise those rights fully and as promptly as possible.

These rights include:

- The right to be informed with fair processing information
- The right of access
- The right to rectification
- The right to erasure
- The right to restrict processing
- The right to data portability
- The right to object
- Rights in relation to automated decision making and profiling

A request for such information is called a Subject Access Request (SAR). Such requests no longer need to be made in writing, irrespective of how the request is made it should be directed to the Headteacher/Head of School of each respective school for it to be attended to.

Any such request will require verification of the person making the request and a record made of that transaction. Ideally for the sake of expediency requests will still be made in writing, supported by proof of identity, such as copy of a driving license or utility bill enabling the Headteacher/Head of School to deal with the request efficiently. We will provide the relevant data within one month from receiving a request.

19. Disclosing Data. (Outside of existing or statutory information sharing agreements)

In certain circumstances the Data Protection Act allows for personal data to be disclosed to law enforcement agencies, such as the police or HMRC without the consent of the data subject.

In such circumstances the Headteacher will disclose the data requested, having first established that

the request is legitimate, and lawful and after seeking legal advice before doing so if necessary.

20. Providing Information

The trust is transparent in the methods it employs to process personal data. This includes:

- Our legal basis for processing personal data
- How data is being used
- How it is shared
- Who is involved in processing it
- How long it is kept
- How to exercise their rights

Appendix A.

Cyber Security Staff Guidance.

Cyber- crime represents a significant threat to the privacy of individuals as well as the commercial success of the trust.

Types of Cyber Crime.

Hackers	Often called vandals, they scan the internet looking for well-known software security gaps. Web servers and email are their favoured target, which they exploit to plant viruses, or use the resources of systems belonging to others for their own means. If no apparent weakness is found they move on to an easier target.
Malware	Refers to various forms of intrusive or hostile computer software, such as viruses, worms and Trojan horses.
Phishing	The fraudulent practice of sending emails, text messages, voice mails or phone calls purporting to induce individuals to enable fraudsters to gain access to personal information, such as passwords, bank account or credit card details. Those details can then be used for criminal purposes.
Ransomware	A type of malicious software designed to block access to a computer system until a sum of money is paid.
Spam	Irrelevant or unsolicited messages sent over the internet to a large number of users, for marketing, phishing or spreading malware.
Spoofing	The creation of an email with a forged sender address. This uses a respectable or reputable email address to hide that the email has been sent by somebody else.
Denial of Service	The use of multiple computers to overwhelm the victim's own computer system to shut down their World Wide Web (www) sites to conventional commercial activity.

Individual Responsibilities
All Teachers, Staff, Contractors, and Volunteers and contracted processors have a duty to:

- Ensure that no breaches or cyber security risks occur as a consequence of their actions
- Ensure the accuracy and integrity of the data they record on the organisations systems
- Take steps to ensure that confidential and sensitive information is stored securely on the system, and encrypted when used on removable media
- Awareness of the various types of cyber and information security incidents and how to report them
- Protect all hardware, software and documents in their care
- Take precautions to avoid the introduction of malicious software on the organisations systems
- Intervene or report any inappropriate use of computer equipment and systems. (Such behaviour constitutes a breach)

Passwords:

- Are confidential and must not be shared with anyone
- Must not be inserted into emails or any other form of electronic communications
- Those applied to user accounts should not be given out
- Are never to be revealed on security forms
- Do not record hints or prompts that help you remember a password
- Must never be shared with anyone
- Must never be written down and kept insecurely
- Must never be stored in a file on a computer or on a mobile device
- Do not use the “remember password” function
- Any suspicion that your password has been compromised must be reported immediately
- Passwords should be at least 8 characters including Capital letters, numbers and where possible one or more symbols (i.e. !£%)

Computer Use.
If you have to leave your desk even for a short time, either log off or ensure that access is denied by a password protected screensaver.

Log off and close down when finishing your working day.

Allowing another individual to use your login to access data for any reason is a breach of the trust’s policy and may contravene the Data Protection Act or the Computer Misuse Act.

You should take reasonable physical steps to prevent your computer or other devices, such as laptops, tablets and the like being accessed unlawfully. Examples include, ensuring doors and windows are kept shut when the office is unoccupied, keeping laptops, tablets and smart phones out of site when being transported, and never leaving them unattended in vehicles overnight.

If you are using a device provided to you by the trust when working remotely, do not permit anybody else including family members to use your device to log onto a web site or social media site for any reason

USB Drives & Removable Media.
Only use devices provided by the trust and only for an educational purpose.

If a colleague or friend share such a device with you or you find one and are intrigued to find out about its contents, do not be tempted to access it on an trust owned computer. You may trust the person sharing the device with you, but the device or their own computer may have a virus.

Bring Your Own device.
You must not download personal data from the trust's system to your own device. This includes capturing images in the workplace or scanning documents.

Email & Malware
Emails can be generated from anywhere around the world, so until you are absolutely sure an email is genuine and its sender credible, do not:

- Click links or open attachments
- Reply to the email, or unsubscribe
- Ring any numbers in the email

How to spot a Phishing Email

- Is your name missing, genuine emails senders personalise the text of their emails with your first name
- Is it requesting personal data or bank details
- Is it unexpected
- Is it something related to a current news event
- If it's from someone you know or a well-known organisation, does it look right, is it phrased correctly
- Is it grammatically correct, or are there spelling mistakes

Identifying Hooks.

- Does the senders address match the organisation that supposedly sent the email
- Hover over the links to show the real destinations
- Contact the sending organisation, using the organisations official website. DO NOT trust or use the contact details or links in the email

Suspicious Activity.
If you identify a suspect email alert your supervisor.

- Do not forward the email
- Do not click the "unsubscribe "links, this alerts the sender that they have located an active email account
- If you have clicked a link that took you to a web site it may be infecting your computer. Tell-tale signs include you being linked to an unrelated or unexpected web site, random activity such as windows opening and closing unexpectedly, if in the slightest doubt turn off the computer, and remove the network cable

Websites.
Browsing infected or malicious websites presents a significant threat. Only browse known and trusted websites.

Remote Working.
You are expected to take exactly the same security precautions when working away from the school, as you do in it. This includes when working in a public space such as on a train or other open area, also when working at home. Measures include ensuring whatever computer, laptop, tablet, smart phone or other type of removable device you are using cannot be unlawfully viewed, accessed, lost

or stolen. Or for personal data processed by the trust to be disclosed or viewed by anybody who is not employed by the trust or authorised to see it.

The software used on the trust's systems are for the purpose of providing education or the administration of our schools, it is not permitted for them to be copied or used for personal reasons. To do so may breach of a licensing agreement as well as contravene the Data Protection Act.

Ransomware.
At any time when Ransomware is found or suspected it must be reported immediately to the Network Manager.

Signs of this type of attack include:

- After opening an attachment or link in an email the performance of your PC starts to slow down
- You are unable to open certain files, and get messages which may say the file type is unsupported, or Windows is unable to open the file
- There are unusual shortcuts on your desk top. Examples used include messages such as "README.html"or README.txt", there are other examples

Malicious Software. (Viruses)
The trust's systems use sophisticated Anti-Virus software countermeasures.

Where a virus is identified or suspected, notify the Network Manager straight away.

Newly acquired discs, magnetic media, DVDs or memory sticks should not be loaded onto computers and other devices used by the trust unless they have been virus checked beforehand. If in doubt seek advice before loading.

Information Security - Staff Guidance

S*tore documents safely, do not take off site unnecessarily.*

E*mails - check recipients or source's address before sending or opening.*

C*hange password frequently - do not share yours with others.*

U*pdate the information and data we hold regularly.*

R*etain information no longer than is necessary.*

E*xclude general access to areas where personal information is in use.*