Sutton Veny CofE Primary School
Data Protection Policy

Introduction:

This policy is written in line with data protection legislation, including the General Data Protection Regulation ("GDPR"), which came into effect on 25 May 2018. This is supplemented by the UK Data Protection Act 2018.
ICO guidance states that 'Schools are data controllers'.

Personal data is defined by the Data Protection Act 2018 as any information which is related to an identified or identifiable natural person.

In school, Staff have access to a wide range of sensitive information, both personal data of staff and pupils, and financial data. Both types of information are managed in a secure way at all times. In order to comply with the Data Protection Act and GDPR, the school will ensure that data is:

- processed fairly and lawfully
- collected for a specified purpose and not used for anything incompatible with that purpose
- adequate, relevant and not excessive
- accurate and up-to-date
- not kept longer than necessary
- processed in accordance with the rights of the data subject
- kept securely
- not transferred outside the EEA (European Economic Area) unless the country offers adequate protection.

In accordance with The Data Protection Act the following types of personal information receive higher level of protection, including information relating to:

- racial or ethnic origin
- political opinions
- religious beliefs or other beliefs of a similar nature
- trade union membership
- physical or mental health or condition
- sexual life (orientation)
- the commission or alleged commission by them of any offence, or any proceedings for such or the sentence of any court in such proceedings.

Information needs to treated securely if loss or disclosure:

- places anyone at risk
- causes embarrassment to an individual or the school
- has legal or financial implications

(see Appendix A)

PROCEDURES AND PRACTICE:

- The amount of data held is reduced to a minimum.
- Data is assessed to consider whether it still needs to be kept or not.
- Personal data is securely stored and sent by secure means.

AUDITING:

- The school is aware of **all** the sensitive data it holds, be it electronic or paper.

- A register of data is kept and updated as necessary (Appendix B)
- How long these documents need to be kept is assessed using the Records Management Toolkit.
- Audits will take place in line with the timetable. (Appendix C).
- This register is reviewed annually to revise the list of data that is held and managed by the school.
- The audit will be completed by a member of staff responsible for data protection.

RISK ASSESSMENT:

The school will regularly carry out a risk assessment to establish what security measures are already in place to ascertain;

- the sensitivity of the data
- the likelihood of it falling into the wrong hands
- the impact of this
- further actions

SECURING AND HANDLING DATA HELD BY THE SCHOOL:

- Any data that is determined to be personal or commercially sensitive in nature will be encrypted. This includes fixed computers, laptops and memory sticks.
- Staff should **not** remove or copy sensitive data unless the media is encrypted, transported securely and stored in a secure location.
- Data should be sent through secure emails with password protection; the password must be sent by other means and not included in the same email.
- Data (pupil records, SEN data, contact details, assessment information) will be backed up, encrypted and stored in a secure place – e.g. safe / fire safe / remote backup.
- All staff computers will be used in accordance with the Teacher Laptop Policy (Appendix D)
- When laptops are passed on or re-issued, data is securely wiped from any hard drive before the next person uses it. This is done our technician using a recognised tool.
- The school's wireless network (WiFi) is be secure at all times.
- Remote access off the school site to any personal data is achieved using an encrypted connection and protected by a username/ID and password. This information is not stored on a personal (home) computer.
- The school will keep necessary pupil and staff information in accordance with the Records Management Society's guidance (see references at the end of this document).
- All staff are trained to understand the need to handle data securely.
- Staff, Governors and pupils sign an annual acceptable use of ICT agreement.
- The school uses an external provider (Shred-it), to destroy any manual information.

REFERENCES:

This policy should be read and understood in conjunction with the following policies and guidance:

The Data Protection Act 2018: http://www.legislation.gov.uk/ukpga/2018/12/section/1/enacted

Data protection: a toolkit for schools August 2018: https://www.gov.uk/government/publications/data-protection-toolkit-for-schools

Records Management Society – Tool Kit for Schools:
http://www.irms.org.uk/resources/information-guides/199-rm-toolkit-for-school

Approved by:	Governing Body	**Date:** 7.2.2022
Last reviewed on:	February 2022	
Next review due by:	February 2023	

APPENDIX A:

Assessing risk of sharing information

1. In case of security breach:
    - Will it affect or identify any member of the school or community?
    - Will someone lose / be out of pocket by / more than £100?
    - Will it cause any kind of criminal case to fail?
    - Is there a risk of discomfort / slur upon professional character of someone?
    - Is anyone's personal safety at risk?
    - Will it embarrass anyone?

If **yes** to any of the questions, the document with include some sensitive information and therefore requires a level of protection.

2. In case of security breach
    - Will it affect many members of the school or local community and need extra resources locally to manage it?
    - Will an individual lose / be out of pocket by £1,000 to £10,000?
    - Will a serious criminal case or prosecution fail?
    - Is someone's personal safety at a moderate risk?
    - Will someone lose his or her professional reputation?
    - Will a company or organisation £100,000 to £1,000,000?

If **yes** to any of the questions additional security should be considered.

APPENDIX B: Register of sensitive data held by the school

Type of data	Held on	Period to be retained	Type of protection	Who can access the data
Pupil SEN data	SENCO laptop and School Server	While pupils are on role at Sutton Veny School – passed on to receiving school	Data is encrypted on laptop	SENCO and Headteacher
Staff Personal Data	School Server	While employed at the school	Data in encrypted	Office Staff and Headteacher
Pupil Personal Data	School Server	While pupils are on role	Data in encrypted	Office Staff and Headteacher

APPENDIX C: Timetable for Information Security Management

Activity	Frequency	Lead
Audit of data held	Annually	Head and admin officer
Encrypting sensitive data	On-going	All staff
Reviewing data backup procedures	Annual	Admin officer
Identifying staff responsible for data security and keep log of names and roles.	Annual	Head
Wiping of laptop data when re-issued	Annual and then when necessary.	ICT Technician
Wiping of laptop data when discarded	As necessary	ICT Technician

APPENDIX D: Staff and Governors Responsible ICT Agreements

Agreement for Responsible E-mail use for Sutton Veny Primary School (Governors, FOS etc.)

1. I will use the email account issued to me in an appropriate way. I will not:
   - access offensive emails or download offensive material
   - make personal use of the e-mail account
   - copy information from the Internet that is copyright or without the owner's permission
   - send e-mails that are offensive or otherwise inappropriate
   - disregard my responsibilities for security and confidentiality
   - access the files of others or attempt to alter the email account settings.
2. I will only access the account with my own name and registered password, which I will keep secret.
3. I will inform the Headteacher as soon as possible if I know my password is no longer secret.
4. I will always log off the system when I have finished working.
5. I understand that the school may, in line with policy, monitor and check my e-mails.
6. If I use removable media, I will ensure that this has been carefully checked to ensure it is free from any type of virus.
7. I will not open e-mail attachments unless they come from a recognised and reputable source. I will bring any other attachments to the attention of the Head Teacher.
8. All joke e-mails and attachments are potentially damaging and undesirable and therefore must not be used.
9. I will report immediately to the Head Teacher any unpleasant material or messages sent to me.
10. Activity that threatens the integrity of the school is forbidden.
11. I understand that if I do not adhere to these rules my email account will be suspended immediately and that other disciplinary consequences may follow.

Name: .....
Signature: ..... **Date:** .....

Agreement for Responsible E-mail, Network and Internet Use for Sutton Veny Primary School (Staff)

1. I will use all computing equipment issued to me in an appropriate way. I will not:
   - access offensive website or download offensive material
   - make excessive personal use of the Internet or e-mail
   - copy information from the Internet that is copyright or without the owner's permission
   - place inappropriate material onto the Internet
   - will not send e-mails that are offensive or otherwise inappropriate
   - disregard my responsibilities for security and confidentiality
   - download files that will adversely affect the security of the laptop and school network
   - access the files of others or attempt to alter the computer settings
   - update web pages etc. or use pictures or text that can identify the school, without the permission of the Headteacher
   - attempt to repair or interfere with the components, software or peripherals of any computer that is the property of Sutton Veny School
2. I will only access the system with my own name and registered password, which I will keep secret.
3. I will inform the Network Manager/School's Technician as soon as possible if I know my password is no longer secret.
4. I will always log off the system when I have finished working. ·
5. I understand that the school may, in line with policy, check my computer files and e-mails and may monitor the Internet sites I visit.
6. If files are to be password protected by my own passwords, I must register the passwords with the Headteacher.
7. If I use removable media, I will ensure that this has been carefully checked to ensure it is free from any type of virus.
8. I will not open e-mail attachments unless they come from a recognised and reputable source.
9. All joke e-mails and attachments are potentially damaging and undesirable and therefore must not be used.
10. I will report immediately to the Headteacher any unpleasant material or messages sent to me.
11. I understand that a criminal offence may be committed by deliberately accessing Internet sites that contain certain illegal material.
12. Activity that threatens the integrity of the school is forbidden.
13. When using social networking sites I will not make 'friends' with pupils, make comments that refer to the school or any persons or events associated with it, or bring the school into disrepute.
14. If an incident is considered to be an offence under the Computer Misuse Act or the Data Protection Act this may be reference for investigation by the Police and could recorded on any future Criminal Record Bureau check.
15. Staff may only use their own technology in school as part of a pre-arranged educational activity, with permission from the Headteacher. Inappropriate use is in direct breach of the school's acceptable use policy.

Name: .....
Signature: ..... **Date:** .....