ST MARY'S CE PRIMARY SCHOOL

E-Data Policy

Signed by:

_____	Headteacher	Date:	_____
_____	Chair of governors	Date:	_____

Statement of intent

The school recognises the importance of data protection and will take the appropriate steps to ensure that electronic data is handled and secured properly.

Review

This policy will be reviewed on an annual basis by the Governing Body, Headteacher and the ICT Co-ordinator in line with any e-security or data protection policies that are in place. The Headteacher has overall responsibility for the implementation of these principles.

Regulation and Practice

This policy will help to ensure that personal data and school data is kept and used correctly and securely, in accordance with the Data Protection Act (DPA) 1998.

Under the principles of the DPA, personal e-data will be:-

- Processed fairly and lawfully
- Obtained and processed for specific or legal purposes
- Maintained adequately and accurately
- Retained only for the time it is required
- Used respecting the rights of the individual
- Effectively secured and monitored

Security and Protection

These measures will ensure that school data is safeguarded from loss or theft.

- Basic measures
    - Passwords are confidential and changed regularly
    - Passcodes are in place for phones / tablets
    - Data stores are in locked areas
    - Computer with sensitive information on are only accessed by specific staff
    - Equipment used by staff at home is logged and processed via a loan system
- Responsible measures
    - A robust, up-to-date firewall software is in place to ensure the protection of the school system through filtering and malware prevention
    - An audit and inventory of all electronic hardware is carried out annually (noting any missing, out-of-date or altered equipment)
    - User privileges are managed and amended where necessary
    - Use of school systems is monitored for safe and professional data use
    - School devices and sensitive folder / documents are password encrypted
- Recognised cyber threats
    - School staff and pupils receive basic information and training on cyber security, enabling them to recognise threatening links or emails that may contact malware
    - Cyber attacks are immediately reported

- Additional e-security measures

  The following systems / procedures may help to avoid or contain data loss or theft:-

  - Intrusion detector system
  - Intrusion prevention system
  - Heuristic threat analysis
  - Penetration testing

Responsible Use

These points will help to ensure that e-data is not misused.

Staff will, in line with the DPA:-

- Handle personal data only after obtaining consent
- Handle sensitive personal or school data with extreme care
- Keep data updated and accurate and delete any out-of-date records
- Never disclose personal data to third parties without consent or other reasonable justification

For best practice:-

- Staff will be trained in pupil safeguarding issues relating to e-data, such as the sharing of personal data, accessing illegal / inappropriate materials, contact with adult strangers / grooming and cyber bullying.

Staff and pupils will be aware of, and if necessary, report:-

- Illegal, harmful or inappropriate texts, photos, videos or games
- Unauthorised access to / loss of / theft of / sharing of personal information
- Any suspicious communication from strangers, including grooming
- The sharing and distribution of personal content without consent
- Cyber bullying, online abuse and aggressive behaviour / threats
- Illegal file sharing / downloading software and other types of copyright
- Inaccurate, falsified or exaggerated online news and media.