|  |  |
| --- | --- |
| : Ava Kennedy School Design | **E-Data Security Policy****“by working together we learn, we achieve, we care”** |

**Policy Consultation & Review**

This policy is available on request from the school office.

This policy will be reviewed in full by the Governing Body every two years. This policy was last reviewed and agreed by the Governing Body on March 2021. It is due for review on March 2023.

Signature:

Headteacher Date:

Signature:

Chair of Governors Date:

**Statement of intent:**

Reedham Primary School and Nursery 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 a two yearly basis by the school management and the IT department 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 guidance:**

This policy will help ensure that personal data and school data is kept and used correctly and securely, in accordance with the General Data Protection Regulations (GDPR)

Under the principles of the GDPR, 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; and effectively secured and monitored.

**Security and Protection:**

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

**Basic measures:** Passwords are confidential and changed bi-annually; passcodes are in place for phones/tablets; data stores are in locked areas; computers with sensitive information on are only accessed by specific staff; and 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an audit and inventory of all electronic hardware and software is carried out regularly (noting any missing, out-of-date or altered equipment); user privileges are managed and amended where necessary; use of school systems is monitored for safe and professional data use; school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 folders/documents are password encrypted.

**Recognising cyber threats:** School staff and pupils receive basic information and training on cyber security, enabling them to recognise threatening links or emails that may contain malware - cyber attacks are immediately reported**.**

**Additional e-security measures:** The following systems/procedures may help avoid or contain data loss or theft: Intrusion detection system, Intrusion prevention system, Heuristic threat analysis, Penetration testing.

**Responsible Use:**

These points for school staff and pupils will help ensure e-data is not misused.

**Staff will, in line with the GDPR:**

* Handle personal data only after obtaining consent.
* Handle sensitive personal or school data with extreme care.
* Keep data updated and accurate, and delete any of out-of-date records.
* Never disclose personal data to third parties without consent or other reasonable justification;
* be conscious of their and the school’s obligations under GDPR in accordance with all of the relevant school policies

**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.