The Angmering School

A Statement of Policy
Guidelines for Acceptable Use of IT and Data

Ambition, Respect, Courage

The Angmering School has adopted the ICO's recommendations ensuring compliance with the General Data Protection Regulation. All members of the school community are given access to use the networked resources available for educational purposes and other school related activities.

This document has been created with guidance from West Sussex County Council. All computer and data users in the school must read this document and agree to it before accessing any school systems. Additionally, all staff must read all documents located in the Google folder 'Data Protection and Acceptable use of IT'. Any changes to the advice and information in this folder is notified to all staff by email and logged on the document 'Log of amendments''

Key Personnel

Governors, the Headship Team, each member of staff and each student in the school have a responsibility for the security of the school's data and equipment.

The Data Manager and IT Services Manager are responsible for the security of data and training all staff in acceptable use of the school's data and resources. Line managers are responsible for ensuring their staff, and teachers are responsible for ensuring their students comply with this policy.

Responsible Use – Etiquette, Safety and Security

- The Data Protection Act should be adhered to regardless of the format of the data storage or communication. This includes electronic, paper and verbal. Personal data should be protected from being accessed by unauthorised individuals.

- All students and staff agree to these conditions of use in this document each time they access any school IT resource or data. Access to resources may be monitored at any time.

- Conditions of use are respected: any breach of the conditions of use may lead to criminal prosecution; in all instances it is considered a disciplinary matter.

- Care should be taken in expressions and opinions relating to any person or organisation in any electronic form of communication and storage.

- Staff and students are expected to use the school's resources for the purposes for which they are made available.

- No-one accesses, creates, transmits or publishes any defamatory material about any person or organisation especially on social media sites.

- All staff to be aware of child protection issues when using social media sites and any other communication method.

- Users are not to download, save, send, photocopy or publish any material that violates copyright laws or the Data Protection Act.

- Users are not to transmit unsolicited material to other users.

- Users are not to attempt to access data and resources on the school network or other systems, including physical storage, by bypassing security or password protection.

- Any software, IT purchases and free software downloads must first be approved by the IT Services Manager. Any procurement made without approval may not be supported by IT support.

- Politeness and use of appropriate language – never send or encourage others to send abusive messages. Report any such messages received.

- Privacy – do not reveal any personal information, such as home address or telephone number, about yourself or others.

- Passwords – do not reveal your password to anyone. If you think someone has learned your password then contact IT support or change it immediately.

- Electronic mail – is not guaranteed to be private. Content is monitored. Messages relating to or in support of illegal activities will be reported to the authorities. Do not send anonymous messages.

- Security – inform ICT Support immediately if a security problem is identified. Do not demonstrate this problem to other users.

- Protection and sharing of information – No student data, including images, are to be published without the appropriate parental consent. The school's management information system holds a record of permissions.

- Protection and sharing of information – Anything you write about an individual may be requested under the General Data Protection Regulation.

- IT equipment disposal is only to be carried out by the IT support department.

- Data Sharing - Personal data is only to be shared by personnel authorised and trained in this responsibility.

- Users are to protect their accounts from ‘phishing’ where logons and passwords are obtained by fraudulent sites appearing like genuine ones. Make sure you only enter your logon details into genuine websites.

- Staff are not to access online school resources containing any personal data on shared devices. Examples of these resources, but not limited to, are Google, SIMS via the VPN and Classcharts..

- Care should be taken when adding your school Google account to your personal mobile phone or tablet. Ensure the account is removed before disposal and do not share the device with anyone as your data will be accessible.

- Staff will be issued with an identity badge allowing quick logon to the photocopiers. Please ensure you keep your badge secure and do not allow students to use it as doing so poses a data protection risk

Limits to the Service Provided

No warranties of any kind, whether expressed or implied, are offered for the school's network service. The school is not responsible for any damages suffered while on the system. These damages include loss of data as a result of delays, non-deliveries, or service interruptions caused by the system or your errors or omissions. Use of any information obtained via the network is at your own risk.

Policy Guidelines:

These policy guidelines were updated 26/11/2020

I agree to the conditions within this document:

Name: _____

Date: _____