Cloud Computing Policy

Prepared/Updated	:	May 2023
Review Frequency	:	2 Years
Next Review Due	:	May 2025

Contents:

Statement of intent

Penwortham Priory Academy recognises the benefits of cloud computing, including those in relation to data processing, value for money and teaching developments.

We are committed to ensuring that the collation, retention, storage and security of all information produced is in accordance with the UK General Data Protection Regulation.

The aim of this policy is to outline the role and responsibilities of staff members, as well as the service provider, in relation to using the cloud for data processing, including educational records, principle's reports and any personnel data.

This policy applies to all staff members, pupils and parents accessing the school's cloud service via personal devices.

1. Legal framework

1.1. This policy has due regard to statutory legislation including, but not limited to, the following:

- UK General Data Protection Regulation (UK GDPR)
- Data Protection Act 2018
- The Freedom of Information Act 2000
- The Privacy and Electronic Communications (EC Directive) Regulations 2003
- Electronic Commerce (EC Directive) Regulations 2002

1.2. This policy has due regard to national guidance including, but not limited to, the following:

- Information Commissioner's Office Guidance on the Use of Cloud Computing (2012)
- DfE (2014) 'Cloud (educational apps) software services and the Data Protection Act'
- DfE (2017) 'Cloud computing services: Guidance for School Leaders'

1.3. This policy is intended to be used in conjunction with the following school policies:

- Child Protection and Safeguarding Policy
- Cyber-security Policy
- Freedom of Information Policy
- General Data Protection Regulation (GDPR) Policy
- Social Media Policy

2. Definition

2.1. For the purpose of this policy, the term 'cloud computing' refers to storing and accessing data and programs over the internet, instead of on a device's hard drive.

2.2. Cloud computing involves schools accessing a shared pool of ICT services remotely via a private network or the internet, resulting in less on-premises equipment and a more flexible, affordable and manageable model of ICT provision.

3. Roles and responsibilities

The school is responsible for:

3.1. Undertaking an ICT network audit to identify enhancements, including those in relation to bandwidth, latency and security, that should be made prior to moving to a cloud-based service.

3.2. Ensuring staff members act in accordance with relevant legislation, including those who process personal information complying with the UK GDPR.

3.3. Organising training for staff members regarding how to effectively and securely use the cloud-based service.

3.4. Collating several quotations for cloud-based service, ensuring that value for money is gained.

3.5. Choosing a reputable cloud service provider, using their self-certification checklist to evaluate their education sector awareness, UK GDPR practices and security controls.

3.6. Ensuring that the cloud service provider has successfully completed the self-certification process.

3.7. Ensuring that there are effective network security arrangements in place.

3.8. Checking that reasonable measures have been taken to cope with the risk of losing, or the disruption of, network connectivity, such as the use of backup internet network links.

3.9. Carrying out privacy impact assessments, when deciding whether to implement new systems, to identity any risks to privacy.

3.10. Making staff members, pupils and parents aware of the expected behaviour when using the cloud service, in accordance with the school's Acceptable Use Agreement.

The cloud service provider is responsible for:

3.11. Keeping their self-certification checklist up-to-date with any changes to the service, ensuring that their existing compliance statement is accurate.

3.12. Ensuring that their self-certification checklist is accurately completed and independently verified by a named senior official of the cloud service provider.

3.13. Promptly providing any additional information or clarification sought by the DfE, as part of the self-certification process.

3.14. Providing clarity regarding the support infrastructure they have in place to assist the school in the event of some serious or unforeseen issue, in relation to the use of their cloud service.

4. Data protection

4.1. All staff members are made aware of the UK GDPR requirements and have an understanding of how these are impacted by the storing of data in the cloud.

4.2. Personal data is processed in compliance with the UK GDPR and the school's General Data Protection Regulation Policy.

4.3. The school's General Data Protection Regulation Policy is adhered to at all times.

4.4. The Data Protection Officer (DPO) will ensure that a contract and data processing agreement are in place with the service provider, confirming compliance with the UK GDPR.

4.5. The school will not use non-managed storage solutions for storing data that is personal or critical to the running of the school.

4.6. The Facilities Manager will ensure that the cloud-based service provider has completed a comprehensive and effective self-certification checklist covering UK GDPR in the cloud.

4.7. The Facilities Manager is responsible for assessing the level of risk regarding network connectivity and making an informed decision as to whether the school is prepared to accept that risk.

5. Monitoring and review

5.1. The use of the school's cloud service will be monitored by the Facilities Manager, with any suspicious or inappropriate behaviour of pupils, staff or parents being reported directly to the DPO and Principle.

5.2. This policy will be reviewed every two years by the School Business Manager and Principle.