ST MICHAEL'S
Church of England High School

Cloud Computing Policy

Contents:

Statement of intent

In our school, our Christian vision shapes all we do. All members of the school community are committed to upholding the St Michael's Church of England Christian values:

- to show love, care and kindness to all in our community
- to value what we have and to share with others
- to enable everyone to achieve their full potential

St Michael's Church of England High School 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 Data Protection Act 1998.

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, headteacher'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.

Signed by:

_____	Headteacher	Date: 28/01/2021
_____	Chair of governors	Date: 28/01/2021

Date of approval	23rd March 2018
Date of review	28th January 2021
Review date	January 2024

1. Legal framework

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

- The UK General Data Protection Regulation (UK GDPR)
- The 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
- DfE (2017) 'Cloud computing services'

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

- GDPR Data Protection Policy
- Freedom of Information Policy
- Online Safety Policy
- Child Protection and Safeguarding Policy
- ITC and Devices 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

3.1. The headteacher is responsible for:

- 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
- informing members of staff whose data will be affected of the school's decision to use a cloud-based service

3.2. The Assistant Headteacher, Facilities and Resources, in conjunction with Managed Service Provider, is responsible for:

- 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
- collating several quotations for cloud-based services, ensuring that value for money is obtained
- ensuring that the chosen cloud service provider has successfully completed the self-certification process

- ensuring that there are effective network security arrangements in place
- 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 back-up internet network links

3.3. The data protection officer (DPO) is responsible for:

- ensuring staff members who process personal information (data controllers) comply with the UK GDPR
- choosing a reputable cloud service provider: using their self-certification checklist to evaluate their education sector awareness, data protection practices, security controls and adherence to local and international data protection laws
- organising training for staff members regarding how to effectively and securely use the cloud-based service

3.4. The data controller is responsible for:

- determining the purposes for and manner in which personal data will be processed
- completing a Cloud service provider suitability checklist to ensure key factors have been considered
- ensuring that the cloud provider only processes personal data for the specified purposes
- reviewing the personal data processed by the school to determine whether or not it should be put into the cloud
- creating a clear record of the data chosen for transfer to the cloud
- considering what data is being collected, whether there is a need for more personal data to be collected and, if so, notifying cloud users of this through a privacy policy
- carrying out privacy impact assessments to identify any risks to privacy or personal data
- complying with the UK GDPR and Data Protection Act 2018

3.5. The cloud service provider is responsible for:

- only processing personal data for the specified purposes
- keeping their self-certification checklist up-to-date with any changes to the service, ensuring that their existing compliance statement is accurate
- ensuring that their self-certification checklist is accurately completed and independently verified by a named senior official of the cloud service provider
- promptly providing any additional information or clarification sought by the DfE, as part of the self-certification process
- 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. The cloud service provider will not process any cloud user's personal data without the consent of the user.

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

4.3. Personal data is processed in compliance with the school's GDPR Data Protection Policy, which is adhered to at all times.

4.4. All files will be encrypted before they leave a school device and are placed in the cloud, and only authorised parties who have the correct encryption 'key' may access them.

4.5. A robust key management arrangement is in place to maintain protection of the encrypted data.

4.6. The loss of an encryption key will be reported to the DPO immediately, failure to do so could result in accidental destruction of personal data and, therefore, a breach of the relevant data protection legislation.

4.7. Data that is 'in transit' will be secured and protected using an encrypted protocol that meets recognised industry standards.

4.8. Personal data that is 'at rest', e.g. stored within the cloud service, will be encrypted.

4.9. The Assistant Headteacher Facilities and Resources will ensure that a contract and data processing agreement are in place with the service provider, confirming compliance with the Data Protection Act 2018 and UK GDPR.

4.10. The data processing agreement will specify the circumstances in which the cloud service provider may access the personal data it processes, such as the provision of support services. Unauthorised access may lead to the inappropriate disclosure, deletion, or modification of personal data.

4.11. If the cloud service offers an authentication process, each user will have their own account. A system will be implemented to allow user accounts to be created, updated, suspended and deleted, and for credentials to be reset if they are forgotten, lost or stolen. Access for employees will be removed when they leave the school.

4.12. An audit process is in place that will alert the school should unauthorised access, deletion, or modification occur.

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

4.14. The Assistant Headteacher Facilities and Resources will ensure that the cloud-based service provider has completed a comprehensive and effective self-certification checklist covering data protection in the cloud.

4.15. The school's data controllers are 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.

4.16. The use of a cloud service will not prevent data subjects from exercising their rights under the UK GDPR or Data Protection Act 2018.

5. Removing data

5.1. The Assistant Headteacher, Facilities and Resources will ensure that the cloud service provider can delete all copies of personal data within a timescale that is in line with the school's Data Protection Policy.

5.2. The Assistant Headteacher, Facilities and Resources will confirm that the cloud service provider will remove all copies of data, including back-ups, are removed if requested.

5.3. The Assistant Headteacher, Facilities and Resources will find out what will happen to personal data should the school decide to withdraw from the cloud service in the future.

6. Monitoring and review

6.1. The use of the school's cloud service will be monitored by the Managed Service Provider, with any suspicious or inappropriate behaviour of pupils, staff, or parents being reported directly to the Assistant Headteacher, Facilities and Resources.

6.2. An audit function will be used to monitor cloud computing procedures and policies to ensure ongoing compliance.

6.3. This policy will be reviewed every three years by the governing board and headteacher.

Appendix 1: Cloud service provider suitability checklist

The following has been considered:	Yes/No?	Further action required
Risks		
Have you made a list of the personal data you hold and how it will be processed in the cloud?		
Confidentiality		
Can your cloud provider provide an appropriate third-party security assessment?		
Does this comply with an appropriate industry code of practice or other quality standard?		
How quickly will the cloud provider react if a security vulnerability is identified in their product?		
What are the timescales and costs for creating, suspending and deleting accounts?		
Is all data in transit encrypted?		
Is it appropriate to encrypt your data at rest? What key management is in place?		
Have you determined the data deletion and retention timescales? Does this include end-of-life destruction?		
Will the cloud provider delete all of your data securely if you decide to withdraw from the cloud in the future?		
Have you found out if your data, or data about your cloud users, will be shared with these parties or shared across other services the cloud provider may offer?		
Integrity		
Are audit trails in place to allow the monitoring of who accesses what data? If so, what trails have been implemented?		
Does the cloud provider allow you to access a copy of your data at your request and in a usable format?		

Has the cloud provider assured you of a timeframe within which they will restore your data (without alteration) from a back-up if it suffered a major data loss?		
The following has been considered:	**Yes/No**	**Further action required**
Availability		
Does the cloud provider have sufficient capacity to cope with a high demand from a small number of other cloud customers?		
Could the actions of other cloud customers or their cloud users impact on your quality of service?		
Can you guarantee that you will be able to access the data or services when you need them?		
Have you determined how you will cover the hardware and connection costs of cloud users accessing the cloud service when away from the office?		
Have you considered how a major service outage at the cloud provider would impact on your business?		
Legal		
Is there a written agreement in place with your cloud provider?		
Have you agreed on how the cloud provider will communicate changes to the cloud service which may impact on your agreement?		
Do you know which countries your cloud provider will host your data in and what information is available relating to the safeguards in place at these locations?		
Can you ensure the rights and freedoms of the data subjects are protected?		
Have you asked your cloud provider about the circumstances in which your data may be transferred to other countries?		
Can your cloud provider limit the transfer of your data to countries that you consider appropriate?		