****

**Longroyde Primary School**

Cloud Computing Policy

Contents:

[Statement of intent](#_Statement_of_intent_1)

1. [Legal framework](#_Legal_framework_1)
2. [Definition](#_Roles_and_responsibilities)
3. [Roles and responsibilities](#_Roles_and_responsibilities_1)
4. [Data protection](#_Data_protection)
5. [Monitoring and review](#_Monitoring_and_review)

## **Statement of intent**

We recognise 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: |  |
|  | Chair of governors | Date: |  |

# Legal framework

* 1. This policy has due regard to statutory legislation including, but not limited to, the following:
* Data Protection Act 1998
* The Freedom of Information Act 2000
* The Privacy and Electronic Communications (EC Directive) Regulations 2003
* Electronic Commerce (EC Directive) Regulations 2002
  1. This policy has due regard to national guidance including, but not limited to, the following:
* DfE (2014) ‘Cloud (educational apps) software services and the Data Protection Act’
* DfE (2017) ‘Cloud computing services’
  1. This policy is intended to be used in conjunction with the following school policies:
* Data Protection Policy
* Freedom of Information Policy
* E-security Policy
* Child Protection and Safeguarding Policy
* Social Media Policy

# Definition

* 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. 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.

# Roles and responsibilities

**The school is responsible for:**

* 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.
  2. Ensuring staff members act in accordance with relevant legislation, including those who process personal information complying with the eight principles of the Data Protection Act 1998.
  3. Organising training for staff members regarding how to effectively and securely use the cloud-based service.
  4. Collating several quotations for cloud-based service, ensuring that value for money is gained.
  5. Choosing a reputable cloud service provider, using their self-certification checklist to evaluate their education sector awareness, data protection practices and security controls.
  6. Ensuring that the cloud service provider has successfully completed the self-certification process.
  7. Ensuring that there are effective network security arrangements in place.
  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.
  9. Carrying out privacy impact assessments, when deciding whether to implement new systems, to identity any risks to privacy.
  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:**

* 1. Keeping their self-certification checklist up-to-date with any changes to the service, ensuring that their existing compliance statement is accurate.
  2. Ensuring that their self-certification checklist is accurately completed and independently verified by a named senior official of the cloud service provider.
  3. Promptly providing any additional information or clarification sought by the DfE, as part of the self-certification process.
  4. 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.

# Data protection

* 1. 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.
  2. Personal data is processed in compliance with the Data Protection Act 1998 and the school’s Data Protection Policy.
  3. The school’s Data Protection Policy is adhered to at all times.
  4. The headteacher will ensure that a contract and data processing agreement are in place with the service provider, confirming compliance with the Data Protection Act.
  5. The school will not use non-managed storage solutions for storing data that is personal or critical to the running of the school.
  6. The headteacher will ensure that the cloud-based service provider has completed a comprehensive and effective self-certification checklist covering data protection in the cloud.
  7. 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.

# Monitoring and review

* 1. The use of the school’s cloud service will be monitored by the ICT Manager, with any suspicious or inappropriate behaviour of pupils, staff or parents being reported directly to the headteacher.
  2. This policy will be reviewed every two years by the governing board and headteacher.