Carville Primary School

ICT Security Policy Statement

May 2018

Revision History

Issue Number	Date	Reason for issue
1.0	April 2018	Implementation of the General Data Protection Regulations (GDPR) coming into force in 2018.

Document Authorisation

Issue Number	Date	Group
1.0	April 2018	Data Protection Officer Senior Information Governance Officer Senior Information Governance Officer

Carville Primary School

Information Security Policy Statement

Carville Primary School is committed to protecting the information of its staff, pupils, governors and other third party organisations. We aim to protect the schools information assets from all threats, whether internal or external, deliberate or accidental.

Carville Primary School will ensure that all information systems operated by our ICT provider are secure and aspire to comply with the requirements of the General Data Protection Regulation (GDPR) and Computer Misuse Act.

Carville Primary School will also ensure that all staff, pupils and Governors fully understand their responsibilities. We aim to achieve this by establishing a culture of care for information held by or on behalf of the school so that any information incident is immediately reported.

It is **Carville Primary School's** Policy to protect information. This will be achieved by:

- Ensuring the confidentiality, integrity and availability of information and information assets belonging to **Carville Primary School** and entrusted to us by our pupils, employees, suppliers, governors, and other third party organisations;

We will do this by:

- Ensuring systems and protocols are in place to ensure information is protected against unauthorised access.
- Ensuring the confidentiality of information is maintained.
- Ensuring regulatory and legislative requirements are met.
- Ensuring a risk based approach is taken to Information Management.
- Ensuring information is protected against unauthorised access.
- Having the right processes in place to ensure the schools ICT Infrastructure is protected and security risks are properly identified, assessed, recorded and managed.
- Ensuring all breaches of information and suspected weaknesses are reported to the Data Protection Officer, investigated and appropriate action taken.
- Ensuring contingency plans are available and tested as far as is practicable to ensure business continuity is maintained.
- Ensuring our staff are appropriately trained.
- Applying a fair and consistent approach to the enforcement of standards of conduct expected from staff and pupils when using social media sites.
- Information is only collected when it is required.

All Headteachers are directly responsible for implementing the Information Security Policy within their school, and for adherence by their staff.

It is the responsibility of each employee to comply with the Information Security Policy, failure to do so may result in disciplinary action.