ICT Security Policy

Governors Meeting:	**21 November 2022**
Safguarding Governor:	**Jane Owens**
Chair of Governors:	**Gail Webb**
Review:	**21 November 2023**

Huxley CE Primary School
ICT SECURITY POLICY

The purpose of this policy is to protect the school's information assets from all threats, whether internal or external, deliberate or accidental.
The aim of this ICT Security policy is to ensure:

- Data confidentiality - No one should be able to view data without need and authorisation.
- Asset Security - The school's physical network and data assets should be protected and made available for use by authorised users only.
- Continuity of school business and minimization of damage by preventing and minimising the impact of security incidents.

It is the policy of Huxley CE Primary to ensure that:

- information is protected against unauthorised access
- confidentiality of information is assured
- integrity of information is maintained
- regulatory and legislative requirements are met
- a Data Breach Policy is produced, maintained, tested and followed
- Information security training is available to all staff.

All breaches of information security, actual or suspected, will be reported to, and investigated by the Headteacher, Mrs Rachel Gourley.

Standards and procedures have been formulated to support the policy, which include:

- Acceptable Use Policy
- data storage and backup procedures
- asset classification and control
- physical and environmental security
- systems development and maintenance.

It is the school's responsibility to ensure the security of their information and ICT assets and data. **All** members of the school community have a role to play in information security.
The Headteacher has direct responsibility for maintaining the policy, standards and procedures and providing advice on their implementation.
It is the responsibility of each member of staff to adhere to the policy, standards and procedures.

The secure handling of school data is everyone's responsibility – whether you are an employee, consultant, software provider, external contractor or managed service provider. Failing to apply appropriate controls to protect this data could be considered to be gross misconduct and may lead to legal action or dismissal.