INFORMATION SECURITY POLICY

Adopted by Kerr Mackie Primary School Resources Committee on **8 May 2018**

To be reviewed by Governors

May 2021

Signed by Chair of Resources Committee

Name: Richard McGinn

Signature:

Date: 8 May 2018

Purpose

The purpose of this policy is to help protect our school against information vulnerabilities and prevent unauthorised access, loss or disclosure.

Scope

This policy applies to anyone who is accessing the schools information, systems and buildings.

Governance

- We will identify someone who will have overall accountability for managing information risks;
- We will ensure our school has a database of information assets and staff accountable for those assets;
- We will ensure our school has a recognised process for identifying and investigating information incidents and breaches - please see incident handling procedure;
- We will ensure information is kept up-to-date and accurate at all times;
- We will ensure information is safely and securely disposed of after it reaches its retention period
- We will have plans in place to ensure the continuity of our school business in the event of an unforeseen incident occurring;

Technical Security

- We will ensure all electronic devices and removable media are encrypted;
- We will ensure staff password protect all electronic devices and never share them;
- We will ensure passwords are changed regularly;
- We will ensure electronic devices and removable media are wiped cleaned and disposed of securely at the end of their use;
- We will make regular back-ups of our data on electronic devices and systems;
- We will protect the schools electronic devices and systems against viruses, malware, malicious codes and cyber-attacks by installing the latest security software;

Remote Working

- If staff working are away from the office, they will only take the minimum physical information required;
- If staff are transporting physical information, they will ensure it is kept out of sight and secure;
- If staff are working from home, they will ensure the schools information is kept private from family members and ensure there is a secure authentication process;

Staff

- We will ensure information is removed and secured from staff leaving employment of the organisation;
- We will consider existing and future access and permission controls for staff, i.e. is it still appropriate for them to have access to the same information if they change positions;
- We will ensure we are satisfied and assured about the people who are working for our school before giving them access to our information e.g. references, vetting, clauses in contracts etc.;

Cyber-attacks	A deliberate exploitation of computer systems, technology-dependent enterprises and networks. Cyberattacks use malicious code to alter computer code, logic or data, resulting in disruptive consequences that can compromise data and lead to cybercrimes, such as information and identity theft
Physical information	Includes paper records and files
Hardware	The physical aspect of computers, telecommunications, and other devices
Software	The various kinds of programs used to operate computers and related devices