Rationale
An Information and Communication Technology (ICT) Security Policy is fundamental to maintaining the integrity of computer security at Findon Primary School. This policy outlines best practices and procedures for day to day security operations.

Aims:
- To increase understanding of security requirements when using the DET computer facilities and services, including leased notebooks as computer networks are intrinsically vulnerable to a spectrum of unprecedented threats.
- To minimise the range of ICT threats and reduce the risks to which Findon Primary School is exposed.
- To increase levels of:
  - Confidentiality - protecting sensitive information from unauthorised disclosure.
  - Integrity - safeguarding the accuracy and ownership of information and computer software.
  - Consistency - have agreed upon expectations of safe use of the internet.
  - Availability - ensuring that information and vital services are available to users when required.
  - Respect for other ICT users.

Implementation
Loss
Loss of confidentiality, integrity and availability of information can occur for a number of reasons:
- Hardware and equipment failure, its storage devices, or the network.
- Software errors.
- Accidents, errors, or omissions by anyone using computers, or the information they process.
- Intentional acts, such as fraud, theft, sabotage, and misuse of information by employees, suppliers, or curious or malicious hackers.
- Environmental hazards, such as fire, storm, dust.

School responsibilities:
- To ensure policies are consistent with and up to date with ICT State and Federal Government Security policies.
- Programs and procedures are put in place to prevent the introduction of viruses and malicious software.
- Information on our Network and SharePoint is password protected.
- The allocation of privileges on our network is controlled. There are two tiers of privilege rights, for all users. Staff have additional rights to access more content that can be used as a teaching tool, for example YouTube.

Individual Responsibilities:
- All users have a responsibility for information security. These responsibilities are described and documented in policies, procedures and job descriptions.
- All users have a unique identifying code to access the network.
- All users have a responsibility to prevent unauthorised access. Staff are password protected to ensure unattended equipment is safeguarded.
- All users must run DET approved antivirus software and set to automatically update.
- All users are strongly advised to back up their work regularly on the school network in their personal drive or on an external device in accordance with best practice, to ensure loss or corruption of data. It is the user’s responsibility as the school doesn’t accept any responsibility for loss of data.
- Staff is advised to check content they show to students before making it available to them through a projected screen. If by chance, unwanted content comes up they must follow the
‘Recommended Actions for Teachers Dealing with Inappropriate Content’ documented in the ‘ICT Acceptable Use’ policy.

- All users immediately inform the Principal or the ICT coordinator on becoming aware of any loss or compromise of information, or any other incident which has ICT security implications.
- All users keep passwords confidential and change their password periodically (as recommended by DET guidelines).
- Users should never log on using someone else’s ID and password.
- It is recommended all users should not allow:
  1. DET computers (including desktops and notebooks) to be connected to open, unencrypted wireless networks at home or in public places.
  2. Use by unauthorised persons.
- All users should be aware that electronic communication is not secure. While every attempt is made to ensure the security of DET ICT systems, users must be aware that this security is not guaranteed, particularly when communicated to an external party.

It is recommended that all staff are to be familiar with this policy, and be aware that further guidelines and details can be found in the DET website.

**EVALUATION:**

- This policy will be reviewed as part of the ongoing policy and process review.

**REFERENCES:**

ICT Acceptable Use Policy
Copyright Policy
Cyber bullying Policy
Media Policy
Privacy Policy