Policy: Staff Use of Laptops

Policy Statement

Jireh Christian School ("the School") staff acknowledge and accept certain responsibilities when they are issued a laptop. Laptops provide the convenience of portability. This convenience exposes the School to certain risks. These include but are not limited to:

1. Theft of School property – laptops are easy to steal and their relatively high value and easiness to sell makes them a common target for theft.
2. Exposure of sensitive data or information – misplaced or unsecured laptops may expose sensitive information to the public. Loss of such data could be utilised by sections of the public for illegal purposes.
3. Damage of School property – laptops can be susceptible to damage both due to their nature and their relatively fragile construction.

Any member of staff issued with a laptop will need to confirm, by signing an acceptance of the policy, that he/she has read, understands and will comply with the policy. A signed copy of the policy needs to be retained at School until the laptop is returned or replaced.

Procedural Guidelines

When a member of staff is provided with a laptop, he/she accepts responsibility for safeguarding the laptop itself as well as the data stored on the laptop. Laptop users are expected to exercise reasonable care and take the following precautions:

1. Recommend that they have appropriate car and house insurance to be able to transport/use the laptop on School business when off site.
2. Take appropriate steps to protect the laptop from theft.
3. Laptops, where possible, should not be left unattended in a parked car. On those occasions when there is no alternative, they should be locked out of sight.
4. Laptops should be carried and stored in a padded laptop computer bag or strong briefcase, that will be provided by the School, to reduce the chance of accidental damage.
5. Laptops should not be used in environments that might increase the likelihood of damage. Staff are to keep an independent record of the laptop serial number. In case of the laptop being lost or stolen, this number will be needed for insurance and Police purposes.
6. Reasonable precautions are to be taken when working on or saving sensitive information (e.g. education records, personally identifiable information, and confidential information)
7. All members of staff are accountable for all network and systems access under their individual user ID. Passwords should be kept secret: they should never be shared with anyone.
8. Laptops are provided for official use by authorised employees. School laptops must not be loaned or be allowed to be used by others.
9. Avoid leaving laptops unattended. Always shut down, log off or lock the screen before walking away from the machine.
10. Anti-virus software is to be kept up to date.
11. Laptops should not be connected to the Internet unless a suitable firewall package has been installed.
12. E-mail attachments are one of the main sources of a virus – staff are to avoid opening any e mail attachment unless they are expected from a legitimate source.
13. Report any security incidents (such as virus infections) to the Principal immediately in order to minimise the risk.

14. Do not download, install or use unauthorised software programmes. No personal programmes are to be used.
15. Any software that is required should be referred to the Principal to ensure correct permissions and licences are in place. A relevant licence will be stored securely for audit purposes.
16. Members of staff must comply with relevant laws, regulations and policies applying to the use of computers and information, e.g., licence, copyright, and privacy laws.
17. The School will not tolerate inappropriate materials such as pornographic, racist, defamatory or harassing files, photographs, videos or e-mail messages that might cause offence or embarrassment. Never store, use, copy or circulate such material on the laptop.
18. Any damage or loss must be reported to the Principal as soon as possible.
19. All staff are to sign a Cyber Safety agreement before they are allocated a device.
20. Failure to comply with this policy could lead to disciplinary action.

Legislative Compliance:

Privacy Act 2020

Review schedule: Triennially

ADOPTED BY BOARD

Date 12th September 2017 Chairperson **R Thornton (Acting)**

Reviewed Date 17th October 2017 Chairperson **W Peat**
Reviewed Date 13th October 2020 Chairperson **M Causley**
Reviewed Date 26th March 2024 Presiding Member **A Coombridge**