Policy for:

ICT Security

Date Written: February 2016

Date Reviewed: November 2023

Next Review Date: November 2023

Signed By: *A. J. Williams*

Governor Responsible for:

Headteacher: Mrs Derries

THE GROVE SPECIAL SCHOOL

I.C.T. SECURITY POLICY

Objectives

1. The objectives of this policy is to create and maintain a high level of awareness of the importance of I.C.T. and data security in school. All staff have a responsibility to ensure proper use of equipment and data within the terms of this policy and any other that may be approved by the school governors.

2. The policy is relevant to all I.C.T. services and electronic communication methods irrespective of the equipment or facility in use and applies to all employees and others using school facilities either on or off school premises.

3. School staff are reminded there are elements of the Staff Code of Conduct which also apply to the proper use of school assets.

Legislation

4. The school and its employees must comply with all UK legislation affecting I.C.T. All school employees must comply with the following Acts, they may be held personally responsible for any breach of current legislation as listed below and any future legislation that may be enacted:

    - Data Protection Act, 2018
    - Human Rights Act, 1998
    - Copyright Designs and Patents Act, 1988
    - Computer Misuse Act, 1990

Violations

5. Violations of this policy will include, but are not limited to, any act that:

    - Exposes the school to actual or potential loss through the compromise of I.C.T. security

- Involves the inappropriate use of equipment, unauthorised disclosure or use of data, and/or the sending or receiving of defamatory or inappropriate material
- Involves the use of data or equipment for illicit purposes, which may include violation of any law, regulation, or any reporting requirement of any law enforcement agency or government body.

6. Computer and data security is viewed seriously by the school and breaches of this policy may result in disciplinary action.

7. Any member of staff who has knowledge of any actual or potential violation of this policy must report it immediately to the Headteacher or Internal Audit at County Hall (01670) 533169.

Passwords

8. The effective use of passwords will protect users from any allegations of misuse. Passwords should be used as a first line of defence against unauthorised use or access to computers and other I.C.T. equipment.

9. Boot and screen saver passwords should be used wherever possible. This is particularly important for portable devices.

10. If a software package comes installed with a default password, that password must be changed immediately after installation.

11. Passwords should not be proper names, birth dates or the word "password". They should be at least six characters long and at least two of those characters should be numeric or punctuation marks. Individual passwords should be used for different applications.

12. Passwords must not be written down or shared unless, this is unavoidable. If access to data or equipment is shared this must be done in the most secure way possible.

13. Passwords should not be the same as a user name or be easily guessed by anyone attempting to log in, especially if they have knowledge of the usual user of the equipment.

14. Passwords must be changed regularly. Where possible changes should be every 30 days, unless otherwise dictated by the system or network.

15. Passwords must not be updated incrementally, e.g. changed by altering only one character of the password.

Unattended equipment

16. Wherever possible, equipment should not be unattended while logged on unless a password protected screen saver has been activated.

Access levels

17. Members of staff will have their access limited only to those systems or data, which they need during their normal employment. If special access is needed for a limited period access rights will be removed after this period has expired. Approval for access to sensitive areas must be given by the Headteacher.

Physical security

18. All desktop devices (PC's, printers and scanners etc.) must have adequate precautions taken to protect them against theft or damage.

19. All portable devices, when not in use, must be retained in a secure environment.

20. All equipment should be security marked (etched, UV pen, etc.) as soon as it is acquired.

21. If portable devices are taken off site, staff must ensure that they take adequate precautions to protect the equipment

against theft or damage at all times. Equipment must never be left in an unattended vehicle.

Security Breaches

22. Any member of staff that becomes aware of an actual or potential breach of security must report immediately to the Headteacher who will then advise Internal Audit.

Software

23. Only software, for which the school holds a legitimate licence, should be installed on any school computer. Licensing arrangements must be followed when installing software.

24. The copying of proprietary software programs or associated copyrighted documentation is prohibited and is a criminal offence. Use of copied software or documentation may lead to personal criminal liability with the risk of a fine or imprisonment.

Viruses

25. Software or files must not be loaded onto I.C.T. equipment unless its source has been verified as legitimate and the software checked for viruses.

26. If discs are used to transfer files, programs or data, they must be virus checked particularly if from an external source.

27. Anti-virus software should be used to protect school equipment and data.

28. If there are any doubts about the authenticity or content of an Email or other electronic data or attachments these must be reported to the Headteacher immediately. Any messages or communications, which are suspicious, must not be opened or loaded on to school equipment until they have been properly checked by an approved member of staff.

End of employment

29. When a member of staff leaves the school, arrangements will be made for the transfer or deletion of any files, programs or software used by that person. Access rights to school systems and data will be removed or reassigned as soon as possible.

Obsolete equipment and files

30. I.C.T. equipment which has become obsolete or surplus to requirement will only be disposed of after any storage media has been cleared of data. Disposal of equipment must be in accordance with Schools Financial Regulations.

31. Discs and other storage media must be disposed of sensitively bearing in mind the content and potential for disclosure.

32. The LEA has arrangements in place for disposal and recycling of obsolete I.C.T. equipment. If you wish to discuss this please contact Merv Brady (01670) 533614.

Telephone and faxes

33. Telephone users must always be aware of their surroundings and take these into account when carrying out any conversation. This is especially important where confidentiality is an issue.

34. No confidential or sensitive documents or information shall be sent by fax unless:

    - The receiving fax machine is known to be secure.
    - The recipient has been advised that the message is being sent and has confirmed that they are available to receive it.
    - The fax message includes a contact name and telephone number should there be any problem during transmission.

35. General disclaimers are not appropriate but should you need to include one on your fax the following should be considered:

    - Contract – This fax is not intended nor shall it be taken to create any legal relations, contractual or otherwise.

- Private opinion – This fax represents the personal views of the author/sender. The author/sender has no authority or delegation to bind the school by this fax and the school accepts no responsibility whatsoever for its contents.
- Confidence – This fax is communicated in confidence. It is intended for the recipient only and may not be disclosed further without the express consent of the sender.

36. All faxes must include the message "If this is delivered to you in error would you please destroy all copies of it immediately and contact the person who sent it".

37. If a fax is received by the school and it is not the intended recipient every effort will be made to inform the sender of this and the recipient should follow the senders instructions, if any, concerning receipt in error.

Email

38. Users must take into account the sensitivity of any data, message or other communication before sending any Email.

39. Email users have a duty to manage this resource in the most efficient and effective way. Saved messages may accumulate which will lead to degradation in service. When Emails are no longer required to be stored, they should be deleted from the computer network or PC.

Use of Email facilities

40. Email facilities are provided primarily for business use however; it is acknowledged that in some exceptional circumstances it may be permissible to respond to a private Email. Regardless of this, school Email facilities must never be used in connection with any secondary business activities.

41. Staff mail boxes and their contents may be examined by the school, the LEA, its auditors or any law enforcement agency. Due consideration of the provisions of the Human Rights Act and any other legislation will be made when undertaking such examinations.

42. Any improper use of internal or external Email, as defined in this policy, or otherwise, may be considered by the school to be a disciplinary matter.

Disclaimers

43. Emails sent using school equipment are sent on behalf of the school and as such the school could be liable for any resulting action.

44. Email the following should be considered:

- Contract – This Email is not intended nor shall it be taken to create any legal relations, contractual or otherwise.
- Private opinion – This Email represents the personal views of the author/sender. The author/sender has no authority or delegation to bind the directorate or authority by this Email and the school accepts no responsibility whatsoever for its contents.
- Confidence – This Email is communicated in confidence. It is intended for the recipient only and may not be disclosed further without the express consent of the sender.

45. All Email should include a "signature":

- Name, Job Title
- School name
- Contact telephone number
- Email address

46. Staff are responsible for the security of their Email facility, Emails will be recorded as having been sent by the person who last logged into the system irrespective of who actually typed and sent the message.

47. The school prohibits the use of Email for purposes, which may be illegal, or the making or sending of Email messages, which may be considered to be offensive in any way.

48. Email must not be used:

- To make possibly defamatory statements about any person or corporate body.
- For sexual or racial or other harassment of any person.
- The generation or dissemination of obscene or blasphemous material.

External Email

48. Users must ensure that they are authorised to send each Email with regard to its content and the recipient.

49. Emails must not bind the school to any position, agree any terms or make any admission unless the Headteacher has first approved them.

50. Staff must not give advice to third parties via Email unless authorised to do so and after having fully considered their own and the school's potential liability.

51. Mail messages sent to other networks should contain the name and job title of the author, the full postal address of the school, the school's telephone and fax numbers and the relevant Email address.

52. The appropriate level of formality must be observed in Emails including the use of appropriate presentation, its use must not be trivialised and it must include the recognised "Email signature".

Email Attachments

53. Where possible, attachments should be password protected, especially sensitive documents. Encryption should also be considered for the sending of sensitive documents.

The Internet

54. Access to the Internet is provided primarily for business use. However, it is recognised that private access may be acceptable in some circumstances provided that it is reasonable, properly

sanctioned by the Headteacher and in the user's own time. Use of the Internet or any other school I.C.T. facility in connection with secondary business activity is strictly prohibited.

55. This valuable school asset must be used in an efficient, effective, ethical and lawful manner. Contravention of this policy may expose the school to legal action or result in action being taken against a member of staff.

56. The school holds no responsibility for any damage or distress caused to users accessing inappropriate or offensive material.

Monitoring of Internet usage

57. The school, the LEA, its auditors and any law enforcement agency may monitor the use of the internet and will report any irregularity to the school governors. Use of the Internet is considered to be an expression of consent by the user to such monitoring, recording and auditing.

58. Systems are in place to restrict access to potentially offensive material, which will record any attempt to access unsuitable sites, and material. These will be investigated and may lead to disciplinary action.

59. Misuse of the Internet may result in disciplinary action, prosecution or, in exceptional circumstances, referral to the Police, and therefore no attempts should be made to access any unsuitable material (pornographic, indecent, illegal, abusive or otherwise offensive images, text or sound).

Copyright

60. Unless there is specific evidence to the contrary, it must be assumed that any material obtained from the Internet is subject to copyright and staff must ensure that they do not breach any copyright.

Data Backup and Disaster Plan

61. The school has a disaster recovery plan, which ensures continuity of service and security of data in the case of emergency or other unforeseen event.

62. Staff and other users are responsible for the backup and protection of data in accordance with this policy.