Barkisland CE (VA) Primary School

Acceptable Use of Digital Technology Policy

Specific Aims of This Policy

The aim of this policy is:

- to communicate clearly to parents, staff, pupils and governors the need for the use of the Internet to be carefully monitored
- to teach all users how to use digital technology safely and appropriately
- to raise awareness of the benefits and risks associated with digital technology
- to set out clearly procedures to follow in any cases of misuse
- to provide a clear framework of sanctions which will be applied with cases of misuse
- to promote communication and co-operation between school and home.

Staff will use the ICT and PSHE curriculum to discuss the safe and appropriate use of digital technology.

General Guidelines for all Users

1. The School Network Software, operated by Calderdale LA, keeps a log of all web-sites visited, the time and date of WWW usage, as well as the user's log-in name for monitoring purposes. This protection deters illegal usage of the Internet, as well as protecting those who comply with this policy.

2. The School Internet connection is through EXA, which acts as a screen and firewall to protect pupils, staff, hardware and software at Barkisland School.

3. All those using machines at Barkisland School to access the Internet undertake to do so in accordance with this policy.

4. The WWW shall not be used to access illegal or inappropriate sites and accidental violation of this rule shall be reported immediately to the Esafety Lead in the first instance. The Esafety Lead shall then report violations with evidence from the Logs to the Headteacher who will then take appropriate action.

5. The WWW shall not be used to plagiarise others work.

6. Any user wishing to download files and programmes should first seek assurances from the Esafety Co-ordinator that the files are compatible with the school network in terms of content and application type. This is to ensure protection for the network as well in terms of software and licence conflict.

7. Staff at Barkisland School reserve the right to check all digital media brought onto the premises with the intention of usage in school machines and to prevent usage where there is a conflict with this policy.

8. School will control access to social networking sites and consider how to educate pupils in their safe use.

9. Emerging technologies will be examined for educational benefit and a risk assessment will be carried out before use in school is allowed.

10. The senior leadership team should note that technologies such as mobile phones with wireless Internet access could bypass school filtering systems and present a new route to undesirable material and communications.

11. The use by pupils of mobile phones is not permitted in school. The sending of abusive or inappropriate text messages or files by Bluetooth or any other means is forbidden.

12. Games machines including the Sony Playstation, Microsoft Xbox and others have Internet access, which may not include filtering. Care is required in any use in school or other officially sanctioned location.

General guidelines for pupils

1. Pupils may only access the Internet or WWW with the permission and supervision of a member of staff.

2. Pupils shall not take part in unsupervised chat, email, or web-conferencing with those outside the school.

3. Any pupil found violating this policy will face the following procedures:
   - the Headteacher and the child's parents to be informed of misuse
   - the child's Internet rights to be reviewed
   - where applicable other agencies may be informed of the violation.

4. Pupils will recognise that using the computer network is a privilege, which could be taken away from them.

5. When using computers pupils will:

   • always behave sensibly, respecting other members of the school

   •only log in using their own username

   • keep their password private

   • never access or distribute any material on the network which may be considered offensive by others or upset them

   • close down any offensive material which has been accessed by mistake and report it to a member of staff

   • be polite at all times, both to those around them and those they contact through the network

• report any offensive messages they receive through the network to a member of staff or the Headteacher

• always seek the permission of a member of staff before downloading any game or other programme

• never give out a full name, address, telephone number, email address or any other details about themselves or anyone else

• only enter the school address after they have got permission from a teacher, and never enter the school telephone number

- never post images taken of themselves or other members of school at school events on the internet.

If any of the rules are broken the matter will be reported to a member of staff as soon as possible and dealt with appropriately.

Pupils in school will read and sign an acceptable use agreement according to their key stage. At the beginning of each school year, parents will be informed of this policy.

Guidelines for staff and governors

Staff will:

1. Sign the school's agreement policy for the acceptable use of digital technology
2. Use the Internet for school and personal interests where these do not conflict with the ethos and interests of the school.
3. Not use the school's Internet facility for financial gain.
4. Recognise their duty to protect the safety of pupils in the use of the Internet and encourage the children in such safe working methods.
5. Report any violation of this policy to the Headteacher and Esafety Lead.
6. Check all website updates with the ICT Co-ordinator for content.
7. Not browse, download or send material that could be considered offensive to colleagues.
8. Report any accidental access to inappropriate materials to the appropriate member of SLT and record on CPOMS.
9. Not download any software or resources from the Internet that can compromise the network, or is not adequately licensed.
10. Ensure all documents are saved, accessed and deleted in accordance with the school's network security and confidentiality protocols.
11. Use encrypted pen drives to store files which may contain personal data pertaining to pupils when working on any machines outside the school network.
12. Network access, including remote access to the server by Ericom, must be made via the user's authorised account and password, which must not be shared with any pupil or person not employed by the school.
13. Respect copyright and intellectual property rights.
14. Ensure that any computer or laptop to be connected to the network or Internet has an up-to-date version of anti-virus software.
15. Ensure they are aware of digital safety-guarding issues so they are appropriately embedded in classroom practice.
16. Ensure that personal information about pupils and staff members will be kept confidential and not revealed through any digital communication.

17. Only open email attachments from known authors.
18. Pupils' names will not be used anywhere on the web site or school twitter account.
19. Not allow unauthorised individuals to access email / internet / intranet.
20. Provide appropriate support for video conferencing
21. Photographs of pupils may only be taken on personal mobile phones under the agreement they are for school use only and are deleted as soon is practically possible e.g. once uploaded onto the school system or printed for school use.
22. Understand that all Internet usage will be logged and this information could be made available to senior management.
23. Agree and accept that any computer or laptop loaned to them by the school, is provided solely to support their professional responsibilities and they will notify the school of any "significant personal use" as defined by HM Revenue & Customs. School laptops will not be used by family members.
24. Only use LA systems in accordance with any corporate policies.
25. Understand that failure to comply with the Usage Policy could lead to disciplinary action.
26. Staff and governors using social networking sites should follow the guidelines provided by the school to ensure they have robust privacy settings. Staff should avoid accepting 'friend' requests from pupils, ex-pupils, parents and former parents.
27. Staff **should not** use social networking sites during PPA or non-directed time.
28. If staff and governors are accessing school emails on their mobile phones a complex password **must** be in place to unlock the phone e.g. combination of letters, numbers and characters.

Guidelines for parents

Parents need to be vigilant in monitoring their children's use of digital technology. All parents:

1. Will be notified of this policy at the beginning of each academic year.
2. Will have available to them on our website the school's eSafety policy.
3. Will only take photographs during school productions for personal / family use. They must not upload such pictures onto the internet, e.g. Youtube or social networking sites.
4. Will support the school approach to online safety and not deliberately post comments or upload any images, sounds or text that could upset or offend any member of the school community or bring the school into disrepute.

The following guidelines give a suggested code for families to follow at home:

- Keep all personal information secret - this includes name, age, sex, home address, landline and mobile numbers, bank details, PIN numbers, passwords and user names. If it is necessary to supply details for registration, or to buy something, your child should always ask for permission and help from you.
- Remember, an online friend is a stranger in the real world so your child should never arrange to meet someone they have met via the Internet without your knowledge and permission. You will go with your child if they do arrange to meet an online friend.
- Your child should not give any indication of their age or sex in a personal email address.
- No one should visit private areas of chat rooms - all chat rooms visited should be moderated and child friendly.
- No one should respond, reply or unsubscribe to unwanted email or spam.
- If your child receives frightening or bullying emails, or any spam with unacceptable content, they should tell you - it is not their fault that they have received them.

If things go wrong:

- Your child should always tell you if anything worries or upsets them.
- You should contact your Internet Safety Provider (ISP) to find out about any child-safety measures they offer and complain to them if your child stumbles upon any inappropriate content or is subjected to any inappropriate contact while online.
- You should install and regularly update filtering software to protect against inappropriate Internet access.

Future Use

1. As the WWW and Internet are in a constant state of development and change, circumstances may arise which are not covered by this policy. In recognition of this the Headteacher/Deputy Headteacher (Current Esafety Lead) is responsible for making day-to-day amendments.

Recording and Reporting

Staff will discuss any concerns during weekly staff meetings.

Offences will be recorded on the school's CPOMS system, which is confidential and for staff information only.

Support staff will report to the Headteacher/Deputy Headteacher (Current Esafety Lead) any concerns relating to Internet misuse.

Any incidents reported to the Headteacher by parents or the wider community will be investigated and dealt with accordingly.

Monitoring and Evaluation

Staff will monitor, through careful observation, the use of digital technology in the classroom and ensure it is in line with the school's acceptable use policy.

Incidences of recorded offences will be formally monitored every half term. Procedures will be reviewed in the light of these monitoring outcomes.

Reviewed by SLT

September 2024