BANCHORY-DEVENICK SCHOOL
A Practice Statement for **Internet Safety**

'The Internet gave us access to everything, but it also gave everything access to us.' James Veitch

Rationale

The Internet and other digital technologies have become an essential part of the lives of young people in today's society, and they form an integral part of everyday life at Banchory-Devenick School. They help raise educational standards, promote pupil achievement, support the professional work of staff, whilst also enhancing the school's management and administrative systems. As part of the statutory curriculum, they are a necessity for effective learning. Access to the Internet is therefore an entitlement for pupils, who need guidance in developing a responsible approach to its use. Children need to learn how to evaluate and judge Internet information, so that they can take care of their own safety and security.

Aims

At Banchory-Devenick School, we aim to ensure that our pupils learn how to use computers, ICT equipment and modern technologies so that they are:

- Able to use digital technologies safely and responsibly to support their learning.
- Know how to use a range of ICT equipment.
- Able to use digital technologies safely and responsibly outside of school.
- Prepared for the constant evolution of technology and can adapt their skills for the future.

Role of Aberdeenshire Council

The school will work very closely in partnership with officers from Aberdeenshire Council to ensure that the schools' policies and procedures are in line with local and national advice and inter-agency approaches to the safety and wellbeing of children and young people.

Aberdeenshire Council is responsible for ensuring:

- The school technical infrastructure is secure and is not open to misuse or malicious attack.
- The school meets required e-safety technical requirements.
- The filtering policy is applied and updated on a regular basis and that its implementation is not the sole responsibility of any single person.
- That they keep up to date with e-safety technical information in order to effectively carry out their e-safety role and to inform and update others as relevant.
- That the use of the network is regularly monitored in order that any misuse/ attempted misuse can be reported to the Headteacher for investigation and action.

Guidelines for Promoting Internet Safety:

1. World Wide Web:
   - If staff or pupils discover unsuitable sites, the URL (address) and a brief description of content must be reported to the school administrator, who will be able to add the site to the school filter list or report it accordingly.
   - The school will ensure that staff and pupils comply with copyright law.
   - Pupils will be taught about the importance of checking the validity of information presented before accepting its accuracy.
   - Staff should be aware that Internet usage can be monitored and traced back to the individual user.

2. Email
   - Pupils may only use approved email accounts on the school system.
   - Staff may only use their work email addresses when communicating with parents/carers and external agencies for school purposes. Care must be taken to ensure that emails are addressed to the correct recipient in order to avoid data protection breaches. BCC should be used if sending an email to multiple recipients.
   - Staff should never share personal email information with children or their families.
   - Pupils must immediately tell a trusted adult if they receive an offensive email.
   - Pupils must not reveal personal details of themselves or others in email communication or arrange to meet anyone without specific permission.
   - If whole class or group email addresses are used in school, this will be monitored by the class teacher.
   - Pupil emails sent to external organisations should be written carefully and authorised by the class teacher before sending.
   - The forwarding of chain mail is not permitted.

3. Social Networking
   - The school uses Twitter to share information and achievements online. Children are unable to post to Twitter and adults should check parental permissions before posting information/photos. Information should be kept general, and children should not be tagged or named.
   - Pupils are actively taught never to give out personal details of any kind which may identify them or their location.
   - Pupils are advised not to place personal photos on any social network space. Instead, they are taught how to use avatars to represent themselves.
   - Pupils are advised on security and encouraged to set effective passwords, deny access to unknown individuals and are instructed how to block unwanted communications.

4. Video Conferencing
   - Video conferencing will always be set up and supervised by a member of Banchory-Devenick School staff.
   - School staff will assess the appropriacy of a video conference in line with pupils age and stage.

5. Electronic Devices

- Pupils should not bring mobile phones, personal tablets or other expensive electronic devices to school or take on trips/visits unless permission has been agreed between the parents and Head Teacher. This will only be granted in exceptional circumstances, and the school will not accept any liability for loss or damage.
- Where possible, staff should not use personal mobiles for work calls. However, it is recognised that this is sometimes unavoidable, e.g. when out on a school excursion. In this instance, staff are permitted to use mobiles, but should hide their number before making the call, e.g. by using *67 before dialling.
- In accordance with data protection regulations, personal devices should not be used to take photographs.
- Staff are permitted to use their own computing equipment to work with, however, NO personal data pertaining to pupil/staff/families may be stored on that system. Similarly, data stored on external storage or removable drives is not permitted unless encrypted/password protected. Staff should be aware that personal computing items, if used for school purposes, are done so at their own risk in terms of damage or loss.

6. The School Website

- The contact details on the website will be the school address, email and telephone number.
- Staff and pupils' personal information will not be published.
- The Headteacher/School Administrator will take overall editorial responsibility and ensure that content is accurate and appropriate.

7. Curriculum

- E-safety should be a focus in all areas of the curriculum and staff should reinforce e-safety messages in the use of ICT across the curriculum.
- In lessons where Internet use is pre-planned, it is best practice that pupils should be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches.
- Where pupils are allowed to freely search the internet, e.g. using search engines, staff should be vigilant in monitoring the content of the websites the young people visit.
- Pupils should be taught in all lessons to be critically aware of the materials/content they access online and be guided to validate the accuracy of information.
- Pupils should be taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet.
- Pupils will be informed that internet use will be monitored.
- A planned e-safety and cyber-bullying programme should be provided as part of Digital Technologies/Health and Wellbeing lessons. This will cover the use of ICT in school and out with. At no time, will online bullying be accepted or tolerated, and pupils will be taught that these behaviours can led to serious consequences.
- Staff should act as good role models in their use of ICT, the internet and mobile devices.
- Children should be taught the SMART rules of internet use:

SMART KIDS

SMART is the message with a simple rule
Better learn this lesson, don't you be no fool.
You can easy stay safe, you can still be cool,
If you wanna be a real SMART kid.

Start with an S, we're talking SAFE to chat,
Keep your personal details underneath your hat.
And you'd better say 'No' if you smell a rat,
If you wanna be a real SMART kid.

M is for MEETING with an online friend,
Take a grown up with you, 'cos they might pretend
They are really like you, but the rules don't bend,
'Cos you wanna be a real SMART kid.

A's for ACCEPTING all the junk email
And if you don't know the sender, then delete or fail.
Just you keep the way clear for your real life pals
If you wanna be a real SMART kid.

R means RELIABLE, here's what we mean
Don't believe just everything you read on screen.
Take a moment to think, and you won't look green
If you wanna be a real SMART kid!

Last comes a T, the letter stands for TELL,
Better blow that whistle. Better ring that bell.
Tell a grown up, a teacher, your folks as well,
If you wanna be a real SMART kid!

(Live Wire Productions)

Appendixes

Useful Websites:

- www.thinkuknow.co.uk
- www.childnet-int.org/safety
- www.bbc.co.uk/onlinesafety/

Useful Documents:

- BD's Parents' Guide to Internet Safety
- BD's Parental Consent Booklet
- SMART rules of the Internet (PowerPoint presentation made by the children in P5-P7)

Useful Staff Training:

The following courses should be accessed through ALDO and it is a staff member's responsibility to ensure their training is kept up-to-date:

- GDPR
- Cyber Security
- Data Protection

March 2023