The Bellbird Primary School

Internet Safety Policy

January 2021

(To be reviewed January 2024)

Our Internet Safety Policy addresses issues of filtering data and Internet monitoring for all users of the school network: both children and adults.

Benefits of the Internet to Education

- Access to worldwide educational resources
- Educational and cultural exchanges between pupils locally, nationally and worldwide
- Staff professional development through access to national developments, educational materials and good curriculum practice
- Communication with support services, professional associations and colleagues
- Access to experts in many fields; for pupils and staff

Use of the internet to enhance learning

- Pupils will be taught to use the internet safely and responsibly.
- Pupils will be educated in the effective use of the internet in research, including the skills of knowledge location and retrieval.
- Pupils will be taught to be critically aware of the materials they read and will be shown how to validate information before accepting its accuracy
- Pupils will be taught to upload and publish their work
- Pupils will be taught to acknowledge the source of information and to respect copyright when using internet material in their own work
- Pupils will be taught to be responsible, competent, confident and creative users of ICT.
- Pupils will use search technologies effectively, appreciate how results are selected and ranked, and be discerning in evaluating digital content
- Pupils will select, use and combine a variety of software (including internet services) on a range of digital devices to design and create a range of programs, systems and content that accomplish given goals, including collecting, analysing, evaluating and presenting data and information

Filtering

We maintain a single point of access to the Internet through a central connection to the County's Internet Service, which is e2bn. At this point a Protex Internet filtering system is maintained to block material that is inappropriate for children. Items filtered include obscene visual images, child pornography and material that are harmful to minors.

It must be noted, however, that due to the nature of the Internet no filtering system is 100% perfect. In response to this, we can ask the County's Internet Service to block additional sites we deem are unsuitable.

Monitoring

Children are allowed to access the Internet when supervised by a teacher or other member of staff. The teacher or staff member supervising the pupil has the primary responsibility of monitoring the pupil's safe and appropriate use of the Internet. It is stressed to them that if ever anything makes them feel uncomfortable on the internet, they should report it at once. For the younger children it is referred to as a "funny feeling in the tummy" which references one of the eSafety films that we use.

The County's Internet Service**, e2bn,** provides a monitoring system that records the Internet sites accessed.

When children enter The Bellbird parents are made aware of "Rules for Responsible Internet Use." Parents are also asked to sign a form allowing the school to put children's work on the school website.

Parents who do not wish their children to use the Internet at school should notify the school in writing.

Live Web Searches

Staff will not use Google to carry out live web searches with children. Children will either be directed to specific websites previously viewed and deemed appropriate by the staff member via a weblink or WebQuest or children will be directed to use Child appropriate search engines, such as http://search.bbc.co.uk/ if the purpose of the lesson is to use Internet search skills.

Messaging

Messaging includes posting text and images to bulletin boards, participating in discussion groups, use of email, and 'chat' features including instant messaging. Children are allowed to use messaging within the class between the teacher and other pupils when this work is part of a school project. All other forms of messaging are prohibited at school.

Responsibility

Each user must take responsibility for his or her use of the computer network and Internet. If a pupil accesses an offensive or harmful site by mistake, the pupil must click on the Home button and report what has happened to a member of staff immediately. Similarly, if a pupil notices another pupil has accessed such a site, they must also report it to a member of staff.

These responsibilities are clearly stated in this policy which is shared by all pupils at the beginning of each school year and revisited by teachers as necessary.

Parental Responsibility

The school will provide all parents of pupils new to the school with this document. This will include a reply slip to show that they have read the information enclosed. The school advises that social media sites are not for children of primary school age and recommends, for Safeguarding and Child Protection purposes, that photographs of children are not named if posted on social media sites.

School Website

The point of contact on the Website will be the school address, school email and telephone number. Staff or pupil's home information will not be published.

The copyright of all material must be held by the school, or be attributed to the owner where permission to reproduce has been obtained.

Pupils' work published on the web will not be identified by their surnames. Including photographs of groups of pupils on the school website can be motivating for the pupils involved, and provide a good opportunity to promote the work of the school. Such photographs will only be used for educational purposes and the identity of children will be protected. The full name of a pupil will never be included alongside the photograph. Parents who do not wish their child's photograph to be used on the school website should notify the school office in writing.

New and Emergent Internet Uses

Emerging technologies will be reviewed for their education value and a risk assessment will be undertaken before use in school is allowed.

Security

We use the County's Internet Network, e2bn, which provides a secure network for the school community.

Confidentiality of Pupil Information

Personal information concerning pupils will not be disclosed or used in any way on the school website without the specific permission of a parent or guardian. Pupils are not permitted to provide private or confidential information about themselves or others on the Internet.

Appendix 1:

The Bellbird Primary School Zoom Meeting Protocol for Bubble Closure Use

Your child has been invited to a 'Zoom class meeting' - hosted by their teacher. As explained in the home learning communication Zoom will be used to get together as a class, learn together, talk about work set and later in the day, review learning.

To ensure that everyone is kept safe, please ensure you read through the guidelines carefully prior to the meeting.

ZOOM CLASS MEETING INSTRUCTIONS AND REQUIRMENTS FOR PARENTS
*Read the following safety guide for parents concerning Zoom:
https://www.saferinternet.org.uk/blog/what-%E2%80%A6-zoom-guide-parents-andcarers#How%20Zoom%20works
*Set up Zoom on your device and if using the APP ensure it has been recently updated.
https://support.zoom.us/hc/en-us/articles/360034967471-Quick-start-guide-for-new-users
*It is advisable to test with friends or family if you haven't used zoom before prior to the first school meeting.
*No recording or screenshots will be permitted.
*You will receive the meeting details for the class ZOOM meeting via an email from school.
*Prior to joining please change attendees name to your child's name – we will then know it is you then in the waiting room. We operate a waiting room to ensure that we have control over who joins the meeting. If we don't recognise the name, we will not be able to admit your child.
*Ensure you (the parent) are able to be within listening distance for the whole meeting to ensure your child is safe and happy. You should not join in with the call, come on to camera once the session has started, unmute or try to speak to the teacher. You should not be on screen apart from at the very start when your child is admitted and the very end when you are leaving the meeting for your child.
*Make sure your child is sitting where there is a blank background, or anything behind your child that you are happy for all other parents to see. You can add a virtual background if needed.
https://support.zoom.us/hc/en-us/articles/210707503-Virtual-Background
*Ensure your child is dressed appropriately – as they would be for a non-uniform day here in school or they can wear uniform if they would like to.
*Explain to your child they will be in a waiting room at first until the host invites them. This might take a while as each person has to be invited in one at a time and we have to check they are who they say they are.
*Ensure you child is present when invited from the Waiting Room and video is switched on – we will be using facial recognition!
*Please ensure you have logged on 5 minutes before the scheduled time.
*Explain to your child that the host (usually the class teacher) will send anyone out of the meeting who is behaving inappropriately.
*Explain to your child the host will be in charge of the sound for everyone and will unmute you when it is your turn to talk. Unless the teachers states you may unmute yourself you should remain muted at all times. This helps sound quality as well as ensuring everyone doesn't talk over one another.
*Explain to your child that the chat function should not be used unless the host directs you to use it.
*Whilst on the zoom call, all school policies apply in regards to behaviour.
*Whenever possible there will be two members of staff on a zoom meeting - if a member of staff's connection drops out they will try to re-join.

APPENDIX 2
Recommendations for Internet use by pupils at home
Personal safety for children when using the Internet:

• It is recommended that parents discuss safe use of the internet regularly with their children. (see our website for more information, including the document “ESafety Support for Parents”).
• Children must know that if anything makes them feel uncomfortable while on the internet, they should tell you immediately.
• Children should never reveal personal information such as their name, home address or phone number or any information that might allow someone to locate them.
• Children should never agree to meet a person face-to-face whom they have “met” on the Internet without their parent’s permission and without an adult being present.
• If someone attempts to arrange a meeting with a child through the Internet, the child must report this communication to their parent or guardian.
• Instant messaging should not be used by children at home unless explicitly approved and supervised by parents.
• Children should choose screen names carefully (e.g. Football_Goals is better than Happy_Sandra10).
• Children should never telephone an online ‘acquaintance’ without parental permission. Caller ID can trace a phone number and from that information, the child's address can be found.
• Nobody should reply to harassing, threatening or sexual messages but should report any such communication immediately to the police.
Parents and children also need to be aware of the legal age limits for use of Social Networking Sites. Eg Facebook

Filtering at home
There are a number of filtering programs that allow parents to block sites and monitor their child’s use of the Internet, including the time of day, number of hours and types of access (such as chat, web, or newsgroup activities). It is recommended that parents use this type of filtering if their child will be using the Internet without direct parental supervision. Filtering can be set to restrict all Internet use when parents are not home.

For more information refer to: http://www.childnet-int.org/ http://www.getnetwise.org/ http://www.safekids.com/

Search engines, such as Google, should be used with extreme caution as the potential for unsuitable sites to be listed is relatively high. At school, the children use http://search.bbc.co.uk/
If using Google for websearches, click on the Preferences button and set your search preferences to Strict Filtering.

Location of Computers in the Home
It is recommended that parents place computers used by children in a heavy traffic area of the home. The best place for a home computer used by a child is in an area such as the living room or kitchen. The worst place is a child’s bedroom. This also applies to Games consoles such as X-Boxes or Playstations, as these provide direct access to the internet and communication with strangers.

Parent / Child Dialogue
It is recommended that parents:
- Have constant dialogue with their child about what they are doing online
- Encourage their child to show them what they are doing
- Consider establishing a "Code for Internet Use" for the home
- Check internet history regularly

Violations
The Internet has much value in today's world and is available in many public places including our libraries. If a child violates the home "Code of Internet Use", it is recommended that parents try to use the situation as an occasion for learning in the first instance, rather than immediately "pulling the plug" on all home Internet access.

Reporting
It is imperative that any illegal or suspicious contact with a child on the Internet is reported to the police immediately.