Ballaugh School E-Safety Policy

If a concern or issue relates to safeguarding or child protection then the Safeguarding and Child Protection Policy and its associated procedures ARE the primary policy until proved otherwise.

Ballaugh School E-Safety Policy

E-safety Policy

E-Safety encompasses Internet technologies and electronic communications such as mobile phones and wireless technology. It states the need to educate children and young people about the benefits and risks of using such technology and provides safeguards and awareness for users to enable them to control their online experiences.

The school's e-safety policy will operate in conjunction with other policies including those for Pupil Behaviour, Bullying, Curriculum, Data Protection and Security.

E-safety - ONLINE

- Access to the internet -

Why is Internet Use Important?

The purpose of Internet use in school is to raise educational standards, to promote pupil achievement and to support the professional work of staff.

The Internet is an essential element in 21st century life for education, business and social interaction.

Internet use is a part of the curriculum and a necessary tool for staff and pupils.

The use of these tools in school and at home has been shown to raise educational standards when appropriately used. However, the use of these new technologies can put young people at risk within and outside the school. Pupils need to learn how to evaluate Internet information and to take care of their own safety and security.

Some of the dangers they may face include:

- Access to illegal, harmful or inappropriate images or other content
- Unauthorised access to / loss of / sharing of personal information
- The risk of being subject to grooming by those with whom they make contact on the internet.
- The sharing / distribution of personal images without an individual's consent or knowledge
- Inappropriate communication / contact with others, including strangers Cyber-bullying
- Access to unsuitable video / internet games
- An inability to evaluate the quality, accuracy and relevance of information on the internet
- Plagiarism and copyright infringement
- Illegal downloading of music or video files
- The potential for excessive use which may impact on the social and emotional development and learning of the young person.

How can Internet Use Enhance Learning?

The school Internet access includes filtering appropriate to the age of pupils. IMAGES CAN NOT BE FILTERED AS THEY DO NOT CONTAIN WORDS TTHAT CAN BE DETECTED BY THE FILTER

Pupils will be taught what Internet use is acceptable, and what is not, and will be given clear objectives for Internet use.

Internet access will be planned to enrich and extend learning activities.

Staff must guide pupils in on-line activities that will support learning outcomes planned for the pupils' age and maturity.

Pupils will be educated in the effective use of the Internet in research, including the skills of knowledge location, retrieval and evaluation.

Our school will ensure pupils have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations acknowledging sources of information used.

Pupils will be taught to be critically aware of the materials they read and shown how to validate information before accepting its accuracy.

- Web filtering -

The school Internet security system is put in place by GTS (Government Technology Services) and includes web filtering. If a pupil encounters inappropriate material, s/he must report it to the teacher and the information should be passed on to the ICT helpdesk (GTS). The teacher must also inform parents about the incident.

3G devices (or other) are currently not allowed into school, as they can bypass web filtering.

- Use of the school's webpage -

Editorial guidance should ensure that the school's ethos is reflected on the website, information is accurate, well presented and personal security is not compromised (GDPR and parental consents). Care must be taken to ensure that all information is considered from a security viewpoint including the use of photographic material.

The contact details on the Web site must be the school address, e-mail and telephone number. Staff or pupils personal information will not be published.

- Email -

Pupils may only use approved e-mail accounts on the school system e.g. IT's Learning messenger and MS Teams. Google docs and Gmail are no longer supported due to security / GDPR reasons.

Pupils must immediately tell a teacher if they receive offensive or upsetting messages.

Pupils should be taught that they must not reveal personal details of themselves or others in e-communications, or arrange to meet anyone without specific parental permission.

Access in school to external personal e-mail accounts is blocked.

Messages sent to external organisations should be forwarded by a teacher.

The forwarding of chain letters is not permitted.

- Social networking sites -

Such sites must not be asked on the school's wifi

In e-safety lessons, pupils learn never to give out personal details of any kind which may identify them or their location.

- Appropriate behaviour -

E-Safety rules must be discussed with the pupils on a regular basis and when accessing the internet.

Pupils will be informed that network and Internet use is monitored and that misuse will result in the facility being removed for a predetermined time, with parents being informed.

Pupils will be taught appropriate and responsible behaviours for using the Internet and communication tools within PSHE and across the curriculum..

Staff will make use of materials from www.thinkuknow.co.uk. and safer schools app.

Pupils will be instructed in responsible and safe use before being allowed access to the Internet and will be reminded of the risks and rules before any session that may involve using the internet.

E-safety will be a focus in all areas of the curriculum where appropriate and staff must reinforce e-safety messages in the use of ICT across the curriculum.

E-safety - Personal Information

- Storage and use of images -

Pupils' full names should not be used anywhere on the website, particularly in association with photographs. Check parental consents on Arbor before taking, or forwarding, a picture for inclusion on the website

Written permission from parents or carers will be obtained before photographs of pupils are published on the school website or used by the media as per annual consents.

Images on a camera or iPad must be deleted when finished with and uploaded to the secure cloud if required for future use.. All data must to be secure (password protected) if being removed from the school building. Staff laptops must be password protected

When taking pictures in the classroom, make sure there are no notices, class lists or details of children in the background.

- Sensitive data -

Personal data should only be recorded, processed, transferred and made available according to the the most up to date GDPR.

- Passwords -

Pupils will be taught about the use of passwords - when to use them, how to make them effective/ strong and about keeping passwords secret.

E-safety - Curriculum

- Education in terms of e-safety for students/teachers/parents -

Pupils will be taught about e-safety as part of their ICT lessons. Teachers must stay current with appropriate information / resources through the Safer Schools App and website.

Parents' are sign posted to the Safer Schools App.

- Delivery of education -

Pupils will be taught as appropriate through ICT e-safety skills lessons, assemblies and cross-curricular topics.

- Differentiation -

Elements of e-safety will be taught at different stages of pupils' school life, according to ability, understanding and the chosen curriculum

E-safety - Devices

- Handheld devices -

iPads are currently provided for use in school under teacher supervision.

- Personal devices -

Pupils must not bring their own devices to school, unless otherwise authorised by the headteacher in consultation with parents. It must be stored securely in the safe and TURNED OFF by the pupil beforehand.

E-safety - Sanctions

- Sanctions -

Sanctions must be inline with the school's behaviour policy. Actions regarding cyberbullying incidents must link with the school's anti-bullying policy? **If a concern or issue relates to safeguarding or child protection then the Safeguarding and Child Protection Policy, and its associated procedures, ARE the primary policy until proved otherwise**.

E-safety - Staff Respinsibilities

- Modelling good practice -

Pupils must see staff using ICT devices in a 'proper' and responsible way.

- Adherence to policy -

All staff are given the School e-Safety Policy. Staff must be aware that Internet traffic can be monitored and traced to the individual user. Discretion and professional conduct are essential.

- Handling e-safety issues -

Complaints of Internet misuse will initially be dealt with by the class teacher, and the headteacher informed.

Any complaint about staff misuse must be referred to the headteacher.

Complaints of a child protection nature must be dealt with in accordance with child protection procedures.

E-safety - Policy Review

The e-Safety Policy relates to other policies including those for bullying and child protection.

- The e-Safety Policy is written by the school, building on guidance from DESC. It has been agreed by senior management and approved by governors.
- The e-Safety Policy and its implementation will be reviewed annually (or sooner if required)

LAST REVIEWED - Sept 2021

Read and understood by (SIGN AND DATE)

.....

.....

.....

.....

.....

.....

.....

.....

.....