e-Safety Policy

E-Safety highlights the need to educate pupils about the benefits and risks of using technology.
It provides safeguards and awareness for users to enable them to control their online experience.
E-Safety depends on effective practice at a number of levels:

- Responsible ICT use by all staff and students

- Sound implementation of e-safety policy in both administration and curriculum, including secure school network design and use.

- Safe and secure internet filtering

Teaching and learning – Why Internet use is important

- The Internet is an essential element for education, business and social interaction. The school has a duty to provide students with quality Internet access as part of their learning experience.

- Internet use is a part of the statutory UK curriculum and a necessary tool for learning for staff and pupils.

- Pupils use the Internet widely outside school and need to learn how to evaluate Internet information and to take care of their own safety and security.

- The purpose of Internet use in school is to raise educational standards, to promote pupil achievement, to support the professional work of staff and to enhance the school's management   functions.

- Internet access is an entitlement for students who show a responsible and mature approach to its use.   **Internet use will enhance learning**   The school Internet access is designed for pupil use and includes filtering appropriate to the age of pupils.

N.B. No Pupils may freely access the Internet. Direct Supervision is in place at all times.

School Responsibilities

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

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

- The school will ensure that the use of Internet derived materials by staff and pupils complies with copyright law.

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

- The schools' internet access will be designed to enhance and extend education.

- Staff should guide pupils to online activities that will support the learning outcomes planned for the pupils' age and ability.

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

- Pupils will be taught to acknowledge the source of information used and to respect copyright when using Internet material in their own work. Pupils will use age-appropriate tools to research Internet content.

Managing Internet Access

- The security of the school information systems and users will be reviewed regularly.

- Virus protection will be updated regularly.

- Security strategies will be discussed with ADEC.

- Access levels to the internet will be reviewed to reflect the curriculum requirements and the age and   ability of pupils.

- Unapproved software will not be allowed in work areas or attached to email.

- Files held on the school's network will be regularly checked.

- The ICT coordinator/network manager will review system capacity regularly.

- The use of user logins and passwords to access the school network

E-mail

Email is an essential means of communication for both staff and pupils. Directed email use can bring significant educational benefits.

- Pupils may only use approved e-mail accounts on the school system for school purposes.

- Pupils must immediately tell a teacher if they receive offensive e-mail.

- Pupils must not reveal personal details of themselves or others in e-mail communication, or arrange to meet anyone without specific permission.

- E-mail sent to an external organisation should be written carefully and authorised before sending, in the same way as a letter written on school headed paper.

- Whole -class or group email addresses will be used in primary schools for communication outside of the school.

- Staff will only use official school provided email accounts to communicate with pupils and parents/carers, as approved by the Senior Leadership Team.

- Access in school to external personal email accounts may be blocked.

Digital Images:

- Digital still and video cameras are used for recording special events as well as being essential tools for everyday learning experiences across the curriculum. As part of pupil induction, parents are asked to sign a consent form for images of their children to be used for school purposes. Some images celebrating the work of pupils involved in everyday and special event activities may be selected to be shown on the school website. **The school will happily remove any image of a child on the school website at their parent's request.**

- Digital images may be shared with partner schools and organisations as part of collaborative learning projects. All such use is monitored and supervised by staff. **We expect all pupils to seek permission from staff before sharing images outside of the school environment.**

Publishing pupils images and work

- Photographs that include pupils will be selected carefully

- Images or videos that include pupils will be selected carefully and will not provide material that could be reused.

- Pupils full names will not be used anywhere on the website, particularly in association with photographs.

- Written consent will be kept by the school where pupils' images are used for publicity purposes, until the image is no longer in use.

Social networking, webcam recordings and blogs

All staff should be made aware of the potential risks of using social networking sites or personal publishing either professionally with students or personally. They should be made aware of the importance of considering the material they post, ensuring profiles are secured and how publishing unsuitable material may affect their professional status.

- The school will block/filter access to social networking sites.

- Pupils will be advised never to give out personal details of any kind which may identify them or   their location.

- Pupils and parents will be advised that the use of social network spaces outside school is inappropriate for primary aged pupils.

- Staff and pupil official blogs will be password protected and run from the
- school   website with approval from the Headmaster. Pupils will be advised on security and privacy online and will be encouraged to set passwords, deny access to unknown individuals
- and to block unwanted communications.

- All members of the school community are advised not to publish specific and detailed private thoughts, especially those that may be considered threatening, hurtful or defamatory

- Staff personal use of social networking, social media and personal publishing sites will be discussed as part of induction.

Cameras, mobile phones and e-safety

Staff should be aware that:

- Staff phones should be on silent and placed in a locker with handbags and other personal effects.

- The school camera or i-Pad must be used when taking photographs in school for educational or   evidence purposes. These photographs remain the property of the school.

- School staff are advised to exercise caution when using social networking sites such as Facebook. It   is unadvisable to add parents as friends on such sites.

Managing filtering

- The school will work with ADEC to ensure systems to protect pupils are reviewed and improved.

- If staff or pupils discover an unsuitable site, it must be reported and blocked

- SLT will ensure that regular checks are made to ensure that the filtering methods selected are appropriate, effective and reasonable.

- The school's broadband access will include filtering appropriate to the age and maturity of pupils.

- The school will have a clear procedure for reporting breaches of filtering. All members of the school community (all staff and all pupils) will be aware of this procedure.

Emerging Technologies

Many emerging communications technologies offer the potential to develop new teaching and learning tools, including mobile communications, Internet access, collaboration and multimedia tools.

A risk assessment needs to be undertaken on each new technology for effective and safe practice in classroom use to be developed. The safest approach is to deny access until a risk assessment has been completed and safety has been established.

- Mobile phones should not be used during formal school time.

- The sending of abusive or inappropriate text messages is forbidden

- Videoconferencing will be appropriately supervised for the pupils' age

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

ICT access

- All staff will be given the School e-Safety Policy and its importance explained.

- Pupils' access to the Internet will be under adult supervision at all times.

- Everyone will be made aware that Internet traffic can be monitored and traced to the individual user

- E-safety rules will be posted in all rooms where there is computer access and discussed with the pupils at the start of each term.

- Pupils will be informed that network and Internet use will be monitored.

- The school will take all reasonable precautions to ensure that users access only appropriate material. However, due to the international scale and linked nature of Internet content, it is not possible to guarantee that unsuitable material will never appear on a school computer. The school cannot accept liability for the material accessed, or any consequences of Internet access.

- All members of the school community will need to be aware of the importance of confidentiality and the need to follow the official school procedures for reporting concerns.

- Complaints of Internet misuse will be dealt with by the Headmaster.

- Any issues (including sanctions) will be dealt with according to the school's disciplinary, behaviour and child protection procedures.

- All members of the school community will be reminded about safe and appropriate behaviour online and the importance of not posting any content, comments, images or videos online which cause harm, distress or offence to any other members of the school community.

Home-School Link

- Parents' attention will be drawn to the School e-Safety Policy in newsletters and on the School Website.

- Parents will be asked to sign and return an Internet access consent form as part of the Home-School Agreement.

- Pupils and parents will be informed of the complaints procedure.

- Parents and pupils will need to work in partnership with the school to resolve issues.

- A partnership approach to e-Safety at home and at school with parents will be encouraged. This may include offering parent evenings with suggestions for safe home Internet use.

- Advice on useful resources and websites, filtering systems and educational and leisure activities which include responsible use of the Internet will be made available to parents.

Network Safety

- The network software prevents changes being made to computer settings.

- Only the network administrators are permitted to install software onto computers.

- All users of the network can be monitored remotely by the network administrators.

E-Bullying

The School takes bullying very seriously and has robust procedures for identifying and dealing with it. E-bullying is the use of any communication medium to offend, threaten, exclude or deride another person or their friends, family, gender, race, culture, ability, disability, age or religion.

Pupils are taught about bullying as part of the PSHE curriculum.

We expect all members of our community to communicate with each other with respect and courtesy.

Bullying of any type will not be tolerated by the school and will be dealt with under the procedures within the Whole School Policies on Behaviour and Anti-bullying.

Copyright

Though there are lots of free to use resources on the Internet, the majority of image, sound and music files are covered by copyright laws. Some can be used for educational reasons without permission provided that the source is stated and that they are not made available outside the school.

Some cannot be used under any circumstances, this is particularly so for music but can apply to other types of file e.g. photographic images.

Care therefore needs to be taken with multi- media work which incorporates anything downloaded from the internet or any other published source that is not uploaded onto the school's website or broadcast through any other technology.

Pupils are taught that the people who put their work on the Internet may not always want people to copy or use their work and that they should check whether they have permission.
We expect all users to respect copyright laws. School e-safety policy

The e-Safety Policy is part of the School Development Plan and relates to other policies

including those for ICT, anti-bullying and child protection.

Date Reviewed: September 2018
Next Review Date: September 2019