Wigginton Primary School
E-safety policy

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

Why is internet use important?

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 information and administration systems. Developing effective practice in internet use for teaching and learning is essential.

The whole school has a duty to provide pupils with access to quality learning using internet technologies and electronic communications and with this, the responsibility to ensure that this learning takes place safely. Pupils are likely to use the Internet outside school and will need to learn responsible computing behaviour to be able to evaluate personal safety.

The school internet access will be designed expressly for pupil use and will include high level filtering provided by our internet service providers. The service uses the leading content filtering solution Smoothwall, and support active and pro-active filtering and monitoring of the internet content. A cloud based version of the Smoothwall filtering is also included.

Teaching & learning

Every year:

- Pupils will be taught what internet use is acceptable and what is not and given clear objectives for internet use.
- Pupils will be educated in the effective use of the internet.
- Pupils will be shown how to publish and present information appropriately to a wider audience.
- Pupils will be taught how to evaluate internet content.
- The school will seek to ensure that the use of the internet derived materials by staff and pupils complies with copyright law.
- Pupils are taught to be critically aware of the materials they read and shown how to validate information before accepting its accuracy.

- Children will be taught the risk of online and cyber bullying, 'stranger danger', social networking and terrorist or extremist material including how to avoid it and what to do if it happens, through assemblies, Computing, PSHE, RSE and RE.
- Parents are informed what their child is being taught and updated through school newsletter.

Managing Internet access

- The school internet access is provided through an agreed management service with City of York council and includes filtering appropriate to the age of the pupils.
- Virus protection is installed on all computers and laptops and is updated regularly.
- All staff and pupils must read the appropriate Acceptable Use Agreement before using any school ICT resource.
- Pupils have separate computer and internet log-ins to staff to limit content access.
- If staff or pupils discover unsuitable sites, the URL (address), time and content must be reported to the class teacher and then to the ICT administrators
- All children must understand that if they see an unacceptable image or text on a computer screen they must report it immediately to a member of staff.
- Rules for safe internet use will be differentiated according to children's age and ability and displayed in every classroom.

Email

E-mail is a quick and easy method of communication, ensuring beneficial and appropriate usage is an important part of e-safety:

- Pupils may only use approved e-mail accounts within the school system.
- Pupils will only be able to send and receive emails through the internal school system
- 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.
- Staff to pupil email communication must only take place via a school email address and will be monitored
- Incoming email should be treated as suspicious and attachments not opened unless the author is known
- Access in school to personal email accounts will be allowed for staff only

Webcams

Webcams can be used to connect with other schools, companies or people. The recipients must be trusted by the staff member who is running the conference.

Webcams may be used to take photos and to film animations and sketches. Images will be used in accordance with the E-Safety Policy and children will not use webcams online unsupervised.

Cameras including video cameras

Children and staff may use cameras and video cameras to record children for educational purposes.
All classes are provided with their own camera which should be used exclusively for school purposes.
Cameras and video recording equipment is not to be taken off school property by any child. It is recognised that staff members may need to work on presentations or video editing which may require taking the device home. See below for acceptable use of data storage.

Data storage and transfer

It is recognised that staff need to store information and transfer data between home and school, including occasional images. The storage of sensitive data is strongly discouraged and it is suggested that such information is sent via email and then deleted. This includes assessment data, images and reports.

Where data of a personal nature is taken home, it must be recognised that this data comes under the General Data Protection Regulations and is subject to the school's GDPR Policy. Care therefore must be taken to ensure its integrity and security. Use of school laptops ensures that data is kept secure within school guidelines and should be used wherever possible. If data is transferred to home computers it must be treated sensitively and removed from the hard drive and any portable device, including USB sticks and memory cards, as soon as is possible.

Mobile Phones

- Mobile phones have access to the internet and picture and video messaging. They present opportunities for unrestricted access to the internet and sharing of images. There are risks of cyberbullying and inappropriate content.
- The sending of abusive, offensive or inappropriate material is forbidden.
- Staff, including students and visitors, are not permitted to access or use their mobile phones within the classroom during teaching hours. They may use them during break and lunch.
- Parents should note that the school accepts no responsibility for the safekeeping of children's mobile phones whilst on the school premises.
- Staff should always use the school phone to contact parents.
- Parent helpers on school trips must not use their mobile phones to take pictures of the children.

The school website

At Wigginton we wish the school's website to reflect our creative approach to teaching and learning. However the school recognises the potential for abuse that material published on the internet may attract, no matter how small this risk may be. Therefore when considering material for publication on the internet we ensure the following:

- The contact details published on the website are the school address, email and telephone number.
- Written permission from parents or carers will be obtained before photographs and names of children are published.
- Pupils' full names will be avoided on the website and blogs, particularly in association with photographs.
- Parents should be clearly informed of the school policy on image taking and publishing, both on school and independent electronic repositories.

Social networking

Pupils

- Access will be blocked to social networking sites through the pupil log-in whilst in school.
- Pupils and parents will be advised that the use of social networking sites outside school brings a range of dangers for primary aged pupils and that only moderated social networking sites should be used for this age range. Parents will be informed that the minimum age for accessing most well-known social networking sites is 13.
- Pupils will be advised never to give out personal details of any kind which may identify them or their location. The use of nicknames and avatars will be advised.
- Pupils will be advised not to place any personal photos on any social networking site.
- Pupils will be advised to look at their privacy settings with an adult to ensure that they are suitable.

Staff

- The school recognises that many staff may actively use social networking sites to communicate socially.
- Although these sites are used by staff in their own time, staff must recognise that it is not appropriate to discuss issues relating to children or other staff via these networks. Staff are encouraged to review their privacy settings to make sure that their profiles and photographs are not viewable by the general public.
- It is never acceptable to accept a friend request from a child from the school. It is also never acceptable to accept as friends ex-pupils who are minors or parents who are not already friends outside of school.
- Staff are required to follow these guidelines and demonstrate acceptable conduct at all times when using the school's IT systems and also act in a professional manner when accessing the internet from home.

Information system security

- Schools ICT systems capacity and security will be reviewed regularly.
- Virus protection is installed and will be updated regularly.
- Only an Administrator from Vital is able to install software onto computers on the school network and add apps to tablets.

Protecting Personal Data

Personal data will be recorded, processed, transferred and made available according to the General Data Protection Regulations 2018.

Assessing risks

- The school will take all reasonable precautions to prevent access to inappropriate material. However due to the international scale and linked internet content, it is not possible to guarantee that unsuitable material will never appear on a school computer. Neither the school nor York City Council can accept liability for the material accessed, or any consequences of Internet access.
- The school should audit ICT use to establish if the E-Safety Policy is adequate, effective or in need of modification and that the implementation of the E-Safety Policy is appropriate.

Managing Emerging Technologies

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

Handling E-Safety Complaints

- Complaints of internet misuse will be dealt with by a senior member of staff.
- Any complaint about staff misuse must be referred to the head teacher
- Complaints of a child protection nature must be dealt with in accordance with school child protection policies.
- Pupils and parents will be informed of the complaints procedure.
- Misuse of the Internet will follow the behaviour policy.
- Issues of internet misuse including cyberbullying will be logged.

Communication of Policy

Pupils

- Rules for Internet access will be displayed in all classrooms and sent home to be read with parents.
- Pupils informed that Internet use will be monitored.

Staff

- All staff to be given the E-Safety policy and its importance explained.
- Staff should be aware that internet traffic can be monitored and traced to the individual user. Direction and professional conduct is essential.

- All staff to read and remain aware of the Acceptable Use Policy.
- Copies of all ICT policies to be kept in registers to be read by supply teachers or volunteers.

Parents

- Parents' attention will be drawn to the school's E-Safety policy in newsletters, the prospectus and on the school website.
- The school will ask all new parents to sign the parent/pupil agreement regarding acceptable Internet use when they register their child with the school.

This policy has been agreed by the Governors and is reviewed annually.

Signed ______________________________ *(Chair of Governors)*

Signed ______________________________ *(Headteacher)*

Date 11.2021

Use Of The Internet By Children

The current computing curriculum makes it essential that children spend some part of their computing lessons working on the Internet. We have agreed a policy for using the Internet which has been approved by all staff who have access to the Internet through the school network and by the school's governors. This policy is designed to ensure that children can safely access information from the Internet.

The rules are: -
1. Pupils must only sign on to the Internet using the username and password supplied by a teacher. Where it is essential that an Internet search is made then a 'child friendly ' engine must be used.
2. Pupils must not knowingly view any material that would normally be considered unsuitable for the school environment.
3. Children should not have access to discussion groups or bulletin boards unless are essential to the curriculum and have been approved by the class teacher, Head and ICT Coordinator.
4. Pupils must not create or transmit material that discredits and insults the good name of others.
5. Pupils should not deliberately violate the privacy of others by reading or copying their personal files.
6. Pupils should not deliberately destroy or corrupt information on the school network unless they have permission to do so (e.g. 'housekeeping' of their own files).
7. Pupils must not use logins and passwords which are not their own.
8. Pupils must not knowingly download or transmit computer viruses.
9. Pupils should listen and follow advice on avoiding viruses.
10. Pupils must not copy other people's work from the Internet and pretend it is their own.

The school accesses the internet using a managed broadband connection. We have an efficient 'firewall' which prevents children accessing a range of sites which we consider unsuitable. Although these are rarely completely foolproof this one does seem to be very efficient.

Children are only allowed onto the Internet when supervised by an adult and must only gain access to the Internet and e-mail with the username and password given to them by a teacher to ensure protection by the 'firewall'. Staff have a responsibility to ensure that their passwords are not given to children.

However, because of the unregulated nature of the Internet there is always a slight risk, however stringent our rules and precautions, that children may view material that we would deem unsuitable for the school environment. Should this situation ever occur then we would: -

- Investigate how it had happened to prevent a reoccurrence
- Work with the parents of the child / children on the consequences of the incident.

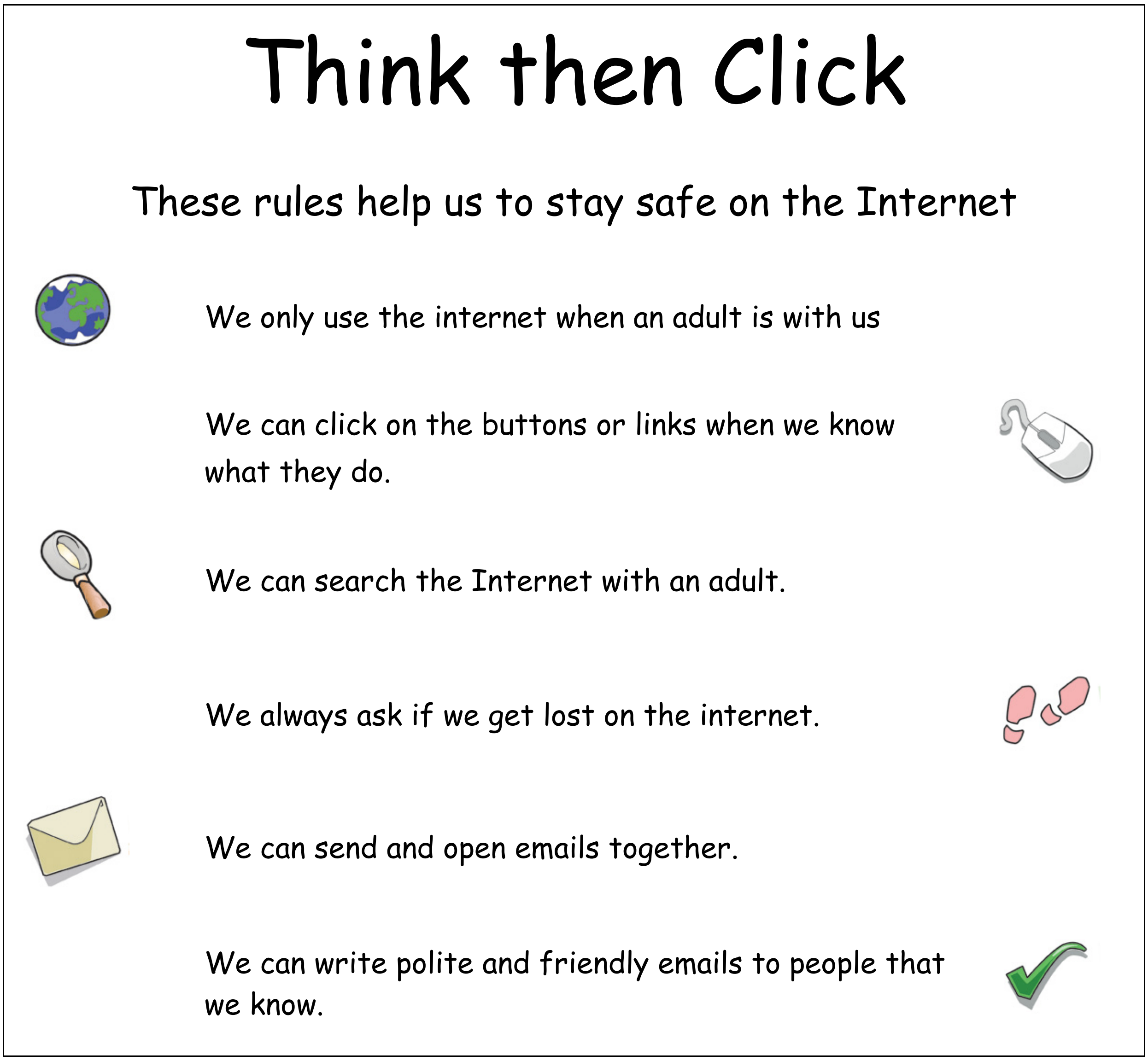
It is essential that parents understand and approve these procedures and I would be obliged if you would return the form below as acknowledgment.

I acknowledge that I have read and approve the rules for use of the Internet. I understand that the school is taking all possible precautions to ensure that no children view unsuitable material when using the Internet as part of the curriculum. However, I also acknowledge that this process is not perfect and, should my child view unacceptable material then I will cooperate with the school to resolve the issue satisfactorily.

Signed . . . .

Name of pupil . . . . Class. . . . .

Key Stage 1



Think then Click

These rules help us to stay safe on the Internet

- We only use the internet when an adult is with us
- We can click on the buttons or links when we know what they do.
- We can search the Internet with an adult.
- We always ask if we get lost on the internet.
- We can send and open emails together.
- We can write polite and friendly emails to people that we know.

Key Stage 2

Think then Click

e-Safety Rules for Key Stage 2

- We ask permission before using the Internet.
- We only use websites that an adult has chosen.
- We tell an adult if we see anything we are uncomfortable with.
- We immediately close any webpage we are not sure about.
- We only e-mail people an adult has approved.
- We send e-mails that are polite and friendly.
- We never give out personal information or passwords.
- We never arrange to meet anyone we don’t know.
- We do not open e-mails sent by anyone we don’t know.
- We do not use Internet chat rooms.