Yenton Primary School

E-Safety Policy

Approved by Governing Body: October 2016

Reviewed and amended: January 2019

To be reviewed: September 2020

Mr Paul Smith

Acting Head Teacher

Yenton Primary School

Chester Road

Erdington

Birmingham

B24 0ED

0121 464 6588

Yenton Primary School
E-safety Policy 2019

Why do we have an e-safety Policy?
We believe that the Internet is an essential part of 21st century life and has a valuable role to play in the education of our pupils. Our school has a duty to provide our pupils with quality Internet access as part of their learning experience. The use of the Internet is part of the National Framework for ICT and the Internet is a useful resource that enhances the teaching and learning taking place within our school. In delivering the curriculum, teachers need to plan for and make use of communications technology, for example, web-based resources and e-mail. Access to life-long learning and employment both increasingly require computer and communications use and pupils need to develop ICT life skills. Home and social Internet use is expanding and it is becoming an important part of learning and communication during leisure time. This brings pupils into contact with a wider range of information, the scope and nature of which may, or may not be appropriate for the pupil. There are also wider dangers that e-mail and chat, telephone conversations and text messages, could all be used as a means of anonymous communication with pupils by adults with inappropriate intentions.
Our pupils use the Internet and ICT on a daily basis and we believe that their e-safety education should start as soon as technologies are introduced.
As a school we recognise that e-safety encompasses Internet technologies and electronic communications, such as mobile phones as well as collaboration tools and personal publishing, which is why we have an e-Policy rather than an Internet Safety Policy. We also recognise that e-safety highlights the need to educate pupils about the benefits and risks of using technology as well as our responsibility to provide safeguards. We need to make all users aware of e-safety and help them to control their online experience. All teachers using ICT in the classroom have a duty to ensure that pupils are reminded about appropriate behaviour regularly. This policy defines the appropriate and acceptable use of the internet by both staff and pupils.

Roles and Responsibilities
The Computing Subject Leader takes responsibility for managing e-safety within our school working in conjunction with the designated Child Protection Coordinator. The e-safety policy and its implementation will be reviewed annually and the school will audit ICT provision to establish if the e-safety policy is adequate and that its implementation is effective. The school's ICT systems capacity and security is managed by Network manager . The ICT technicians will ensure that virus protection is updated regularly and take responsibility for Firewall and antivirus software. Teachers are responsible for the virus protection on their laptops.

E-Safety Education
We will continue to ensure that the school's Internet access will be designed for our pupils' use and will include filtering appropriate to the age of pupils. E-safety lessons will form a regular part of the children's education both within the discrete teaching of ICT and when the Internet is used across the curriculum. Our pupils will be taught when Internet use is allowed; what Internet use is acceptable and will be given clear learning objectives related to Internet use. The children will be taught rules that will help to protect them when using the Internet both at school and at home. We will also provide parents with information about e-safety both through newsletters and the school website.

Our Pupils
Pupils will only be allowed to use the internet when supervised by teaching staff and teaching assistants and when asked to do so. Pupils will be required to log on to the internet using their own

logins and passwords. Pupils will only use email in school when supervised by adults and when instructed to do so. Pupils will be taught not to reveal any personal details of themselves or others in any communication.

The School Website
The point of contact on the Web site is the school address, admin e-mail address, School Business Manager and the school telephone number. Staff or pupils' home information will not be published. We want our school web site to reflect the diversity of activities, individuals and education that takes place at Yenton Primary School. However, the school recognises the potential for abuse that material published on the Internet may attract, no matter how small this risk may be. Photographs of children can only be published to the website with the parents' written permission. Pupils' full names will not be used anywhere on the website, particularly associated with photographs. The Headteacher and Web Administrators will take overall editorial responsibility and ensure content is accurate and appropriate.

Filtering
The school will ensure that filtering of websites is done appropriately. Filters can be applied by the Web Administrator within school but are also managed by Birmingham Local Authority that monitors and blocks inappropriate content in school. Unfortunately there is no software that is 100 % successful and on the rare occasions we have had breaches, there is a very thorough procedure that is followed, as set out in our e-safety policy. Any incident is always reported to parents in writing, so please do not be concerned . If staff or pupils discover an unsuitable site, it must be reported to the e-safety Coordinator. The ICT Coordinator will ensure that regular checks are made to ensure that the filtering methods selected are appropriate, effective and reasonable.

Social Networking
Social networking Internet sites (such as, Twitter, Facebook) provide facilities to chat and exchange information online. This online world is very different from the real one with the temptation to say and do things beyond usual face-to-face contact.

- Use of social networking sites and newsgroups in the school, is not allowed and will be blocked/filtered.
- Pupils will be advised never to give out personal details of any kind that may identify themselves, other pupils, their school or location. This will also include not using personal photographs and videos.
- Pupils and parents will be advised that the use of social network spaces outside school is inappropriate for primary aged pupils.
- Pupils will be encouraged to only interact with known friends, family and staff over the Internet and deny access to others.
- Parents, pupils and staff will be advised of the dangers of discussing pupils, staff or the school on social networking sites. The governors will consider taking legal action, where appropriate, to protect pupils and staff against cyber bullying and defamatory comments.

Mobile Phone Usage
Yenton School recognises that parents may wish their children to have mobile phones for use in cases of emergency. Many new mobile phones have access to the Internet and picture and video

messaging. Whilst these are the more advanced features, they present opportunities for unrestricted access to the Internet and sharing of images. There are risks of mobile bullying, or inappropriate contact.

Mobile Phones (children)

Unfortunately, there are currently now instances of mobile phone camera images being used inappropriately to bully children in other schools. This policy will hopefully prevent such issues affecting our school.

It is the school expectation that children do not have access to mobile phones or are allowed to bring mobile phones to school, or take them on school trips. If a parent believes there is an exceptional circumstance that requires a child to carry a mobile, they should write to or contact the class teacher explaining the situation.

If it is agreed that there is a valid reason for the child to carry a phone, then the mobile phone is handed in to the office at 8.55 by preferably the parent and then be recollected at 3.30. The phone is then locked away in the office until collection.

Mobile Phones (adult)

There are situations in schools where adults have been accused of taking photographs of children using their mobile phones, thus creating child protection issues. To protect staff from such allegations and to maintain professional standards, this policy will satisfy these issues.

Staff are allowed to bring mobile phones on site, but must be turned off/ be on silent mode and not visible in any area where children could usually appear (i.e. classrooms, halls, library, school office,playgrounds and ICT suites). Phones can be kept on silent, but should be kept in a locked bag or cupboard, in order to protect it from theft.

Under exceptional circumstances, a member of staff can request that their phone be turned on and accessible/ visible during the school day. Such a case needs to be discussed with the Head Teacher.

During breaks staff are obviously allowed to check their phones and make calls if necessary, but this must be in areas where children would not be able to enter (i.e. Staff room, a manager's office). This does not include shared areas in case children are working on jobs.

Mobile Phones and Visitors

All visitors should likewise follow this policy and if a member of staff is concerned re their use of their mobile phone, or has a child reported a concern, please inform a senior manager immediately, who will then have to request to examine the phone.

Some engineers (e.g. Promethean) as part of the contract with the school are permitted to carry mobile phones, in order to photograph their working conditions. This is agreed beforehand, but nonetheless any concerns must be reported and a senior manager is allowed to search the phone for images. Likewise, the Site Supervisor is also allowed to carry mobile phones, but should wherever possible, answer the phone in a private place.

Out of professional courtesy, mobile phones should be turned off during staff meetings, unless an agreement has been made with the Head Teacher.

Mobile Phones On Trips

On a normal school day trip, it is expected that staff will carry the school mobile phone. If the year group are going away for more than one day or are spread over 2 buses, then it is understood that staff would need to take their own phones to stay in touch with each other.

In this circumstance to protect the staff members it is important to consider where and how you are using your phone. It may be advisable to use the phone near to another member of staff/ adult if children are present, or to make the phone call away from the children, whilst making sure that the children are still supervised by a member of staff.

Video Recorders and Cameras.

In order to protect staff from any sort of allegation, staff should not use their own cameras or video cameras to record the children in school.
The school has cameras and these should always be used.
Images once used, printed or developed should be removed from laptops. Particularly special photographs can be 'burned' onto disk and then handed to the school secretary to keep for the school prospectus.
Whenever taking photographs, staff must always check the register of pupils who have been refused permission by their parents to have photographs taken of them. Staff should be then aware of how they use such images.
Parents, legal guardians, family members and friends can take images of their child and friends participating in school activities for family and personal use.
Images will only be taken at the end of the performance as directed by the member of school staff and must not be recorded during the performance itself. If this does occur , the person taking the image will be asked to stop, and if they continue then they will be asked to leave the school premises.

Acceptable Use
All staff must read and sign this e-safety and Acceptable Use Policy before using any school ICT resource. The school will keep a record of all staff and pupils who are granted Internet access. The record will be kept up-to-date, for instance a member of staff may leave or a pupil's access be withdrawn. Users are managed by the Internet Administrator in accordance with the e-safety Coordinator.

All Internet activity should be appropriate to staff professional activities or the children's education. Access to the Internet within school is limited to the use of authorised accounts and passwords, which should not be made available to any other person. Each member of staff has their own Internet login details which should be kept private. There is a separate logon for each year group within school. Activity that threatens the integrity of the school's computer systems, or that attacks or corrupts other systems, is prohibited. In regards to e-mail, users are responsible for all e-mail sent and for contacts made that may result in e-mail being received. Due regard should be paid to the content. The same professional levels of language should be applied as for letters and other media. It is the responsibility of the user to ensure that they have logged off the system when they have completed their task.
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.
Children must not be given unsupervised access to the Internet. For the purposes of this policy, "supervised" means that the user is within direct sight of a responsible adult. All of the pupils should be regularly reminded of the School's Internet Rules.
Procedures to follow in case of an incident involving inappropriate information being accessed by children or staff.

If there is an incident in which a pupil is exposed to offensive or upsetting material the school will wish to respond to the situation quickly and on a number of levels. Responsibility for handling incidents involving children will be taken by E-safety leader.

- There is a recording sheet that is used with a step by step guide to indicate the procedure to follow if inappropriate websites are viewed (these sheets are near every computer in school – appendix 1)

- Staff must ensure that they turn off the monitor and not the computer, as the e-safety leader or technicians may need to examine the pc.
- If one or more pupils discover (view) inappropriate material our first priority will be to give them appropriate support.
- The pupil's parents/carers will be informed and given an explanation of the course of action the school has taken through a standard letter (appendix 2 and 3). The school aims to work with parents/carers and pupils to resolve any issue;
- If staff or pupils discover unsuitable sites the e-safety/ IT Co-ordinator will be informed. The IT Co-ordinator will report the URL (address) and content to the Internet Service Provider and the LEA; if needed the ICT coordinator will also block the through informing the LEA.
- If it is thought that the material is illegal, after consultation with the ISP and LEA, the site will be referred to the police.
- Any issue relating to E-Safety will be informed to parents on the same day through a standard letter (appendix 2) thus ensuring parents are fully aware that staff have dealt with the situation.
- If pupils abuse the privileges of access to the internet or use of e-mail facilities by failing to follow the rules they have been taught or failing to follow the agreed search plan when given the privilege of undertaking their own internet search, then sanctions will be taken. This may involve a warning at first, before then informing the parents/carers. Teachers may also consider whether access to the internet may be denied for a period.

Minor incidents may involve pupils;

- Downloading irrelevant material deliberately, in breach of the acceptable use policy.
- Misconduct associated with student logins, such as using someone else's log in or password.

All such incidents of inappropriate use or misconduct must be logged by the E-Safety coordinator.

All staff will be given the school e-safety policy and the importance of the policy will be clearly explained. The e-safety policy will be available on the school website for both teachers and parents to access. All staff should be aware that Internet traffic can be monitored by the Internet Administrator and can be traced to the individual user. Discretion and professional conduct is essential.

Parents' attention will be drawn to the School e-safety Policy in newsletters, the school brochure and on the school Website. We have also created a page to support parents in using ICT at home with their children safely. We hope that taking an active role in providing parents with information and guidance about e-safety we will further protect our pupils and help to ensure that they are getting e-safety messages in the home too. We realise that parents and carers have a key role in promoting e-safety at home. ICT offers the opportunity for children and parents to learn together and e-safety is a topic which can be taught at home and school.

Policy Adoption, Monitoring and Review

Policy adopted by Governors on: _____

Policy last reviewed on: _____

Policy due for review on _____:

This agreement covers use of digital technologies in school: i.e. **email, Internet, intranet and network resources**, software, **equipment and systems.**

- I will only use the school's digital technology resources and systems for Professional purposes or for uses deemed 'reasonable' by the Head and Governing Body.
- I will only use the approved, secure school email system for any school business.
- I will not browse, download or send material that could be considered offensive to colleagues.
- I will report any accidental access or receipt of inappropriate materials, or filtering breach to the e-safety coordinator.
- I will not allow unauthorised individuals to access email / Internet / network, or other school systems.
- I will not download any software or resources from the Internet that can compromise the network, or are not adequately licensed.
- I understand that all Internet usage and network usage can be logged and this information could be made available to my manager on request.
- I will not connect a computer, laptop or other device (including USB flash drive), to the network / Internet that does not have up-to-date anti-virus software, and I will keep any 'loaned' equipment up-to-date, using the school's recommended system.
- I will not engage in any online activity that may compromise my professional responsibilities.
- I will ensure any confidential data that I wish to transport from one location to another is protected by encryption and that I follow school data security protocols when using any such data at any location.
- I will ensure I am aware of digital safety-guarding issues so they are appropriately embedded in my classroom practice.
- I understand that failure to comply with the Acceptable Use Policy could lead to disciplinary action.
- I confirm that I have read and understood the **Yenton Primary School E-Safety and Acceptable Use Policy.**

- Any content I post online (including outside school time) or send in an email will be professional and responsible and maintain the reputation of the school.

- To protect my own privacy, I will use a school email address and school telephone numbers as contact details for pupils and their parents.

- I will not use my personal mobile phone or other personal electronic equipment to photograph or video pupils.

- I will take all reasonable steps to ensure the safety and security of the school ICT equipment which I take off site and will remove anything of a personal nature before it is returned to the school. I confirm that I have read the school **ICT Equipment Risk Assessment and Data Security Policy** and that I will use all means of electronic communication equipment provided to me by the school and any personal devices which I use for school activity in accordance with the document. In particular:

- I will take all reasonable steps to ensure that all laptops and memory devices are encrypted (memory sticks) fully virus protected and that protection is up to date.

- I will report any accidental access to material which might be considered unacceptable i
- immediately to the Deputy Head or Headteacher and ensure that it is recorded.

- Confidential school information, pupil information or data which I use will only be stored on a device which is encrypted or protected with a strong password. Computers will have a password protected screensaver and will be fully logged off or the screen locked before being left unattended.

- I understand that I have the same obligation to protect school data when working on a computer outside school.

- I will report immediately any accidental loss of confidential information so that appropriate action can be taken.

- I understand that the school may monitor or check my use of ICT equipment and electronic communications.

User Signature
I agree to abide by the school's most recent E-Safety and Acceptable Use Policy 2016
I wish to have an email account; be connected to the school shared drive, Internet and be able to use the school's Computing resources and systems.
Signed:.....
Date:.....
Full name:.....
Job title:.....
Authorised Signature (Acting Headteacher)
I approve this user to be set-up
Signed:.....
Date:.....
Full name: Paul Smith

Appendix 1 Safety Record Log Sheet

Date _____ Time_____

Member of staff present _____

Venue_____

Website on _____

Children who view image/ issue:

_____

_____

Action taken by Teacher:

Informed parent of action? Yes / No

Informed E safety Coordinator? Yes / No

Informed ICT Leader? Yes / No

Counselling given to child? Yes / No

Other action taken:

Appendix 2 – Letters to Parents

INTERNET SAFETY

Date: _____

Dear _____,

Your child has today been working on the internet during normal lessons. Unfortunately, through no fault of their own, your child witnessed inappropriate images/ language on one of the webpages they were visiting. The children were:

The school takes internet safety very seriously and the incident has been dealt with in accordance with our e-safety policy. The incident has been recorded and if possible, we will block the website. The children involved have had the incident discussed with them and they have been re-assured in the matter.

All the webpages we access are filtered by a system run by Birmingham City Council, but unfortunately images can sometimes slip through.

It is important that the children do realise that in the real world when they are on computers at home or elsewhere, away from school filters, that the internet can be a dangerous place. Such dangers are regularly discussed within the school ICT curriculum and we do held an annual assembly in the school to identify and talk about such concerns.

I am very pleased that your child acted so sensibly, in reporting this incident to a member of staff. This has enabled us to deal with it appropriately.

If you should want to discuss this further with me, please do not hesitate to contact me.

Thank you for your support,

Mr P Smith
Acting Headteacher.