St Winifred's RC Primary School

E-Safety Policy

Written by: Mr T Hanvey
Updated: March 2015

What is e-safety?

E-safety encompasses not only internet technologies but also electronic communications such as mobile phones and wireless technology. It highlights the need to educate children and young people about the benefits, risks and responsibilities of using information technology. It provides safeguards and raises awareness to enable users to control their online experiences.

Writing and reviewing the policy.

- The policy has been written by the school, building on local authority and government guidance. It has been agreed by the senior management and approved by governors.
- The e-safety Policy and its implementation will be reviewed annually.

The use of the internet in school

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 use is part of the statutory curriculum and a necessary tool for learning.
The internet is an essential element in 21st century life for education, business and social interaction. The school has a duty to provide students with quality internet access as part of their learning experience.

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

The school internet access is designed expressly for pupil use and includes filtering appropriate to the age of pupils.
Pupils will be taught what internet use is acceptable and what is not and given clear objectives for internet use.
E-Safety lessons are now in place in all year groups.
Staff should guide pupils in on-line activities that will support the learning outcomes planned.
Pupils will be educated in the effective use of the internet in research, including the skills of knowledge location, retrieval and evaluation.

Procedures for Use of a Shared Network

Users must access the network using their own logons and passwords. These must not be disclosed or shared.

Users must respect confidentiality and attempts should not be made to access another individual's personal folder on the network without permission.

Software should not be installed without prior permission from T Hanvey, Computing Subject Leader / E-Safety Co-ordinator.

Machines should be logged off/locked if they are unattended.

Procedures for Use of the Internet and Email

Users must access the internet and email using their own logon/password and not those of another individual. Passwords must remain confidential.

The internet and email should only be used for professional or educational purposes.

Children must be supervised at all times when using the internet and email.

Accidental access to inappropriate, abusive or racist material is to be reported without delay to the E-Safety Co-ordinator or Headteacher who will arrange for the URL to be blocked.

Internet and email use will be monitored by the Local Authority.

All emails sent should be courteous and the formality and tone of language appropriate to the reader. No strong or racist language will be tolerated.

All emails sent from the school email accounts will carry a standard disclaimer disassociating the school and the Local Authority with the views expressed therein.

Bullying, harassment or abuse of any kind will not be tolerated.

e-safety posters are to be displayed around the school informing children of good practice.

Staff Usage and access of You Tube

Staff currently have access to 'You tube' and should note that advertisements will show up that may not be age appropriate therefore they must always preview each clip used before sharing with children.

Procedures for use of instant messaging, chat weblogs and social media.

The use of instant messaging (e.g. MSM messenger) is not permitted

Staff and pupils may not access social networking websites via the school network. This includes Twitter, Facebook, Instagram, What's App and Snapchat.

Children and staff are encouraged to join in forums hosted on the VLE but are reminded of the safe practices and behaviours to adopt when posting material as well as the need to be polite at all times.

Weblogs and chat rooms may be available to pupils via the VLE. These will have a strict code of conduct and pupils judged to be misusing these will be blocked from having further access.

Procedures for use of cameras, video equipment and webcams

Permission must be obtained from a child's parent or carer before photographs or video footage can be taken. The office holds a list of permissions which staff should check before using equipment.

Photographs or video footage will be immediately downloaded onto the network and deleted from the camera or video recorder.

Any photographs or video footage stored on the network must be deleted once no longer needed.

Only school staff may be permitted to use cameras or video equipment during a trip or visit.

Where possible school equipment should be used. If, however, a staff member uses their personal equipment they must download the photographs or footage to the school network at the earliest possible opportunity and delete it from the camera or video recorder.

Webcams must only be used with an adult present and must be turned off and facing the wall when not in use.

Procedures to ensure safety of the school's website and VLE

The school website is now a limited site which does not hold photographs or video footage of the pupils.

All changes to the website must be approved by The Head-teacher and Mr Hanvey

User names and passwords for updating the website are held by the Mr Hanvey.

Overall responsibility for the VLE lies with Mr Hanvey who is the site administrator and is responsible for monitoring the content and use of the VLE.

Teachers may upload files, photographs, video footage and weblinks to the VLE in their own class area adhering to the procedure for using a camera or video equipment.

Images and files uploaded must not be in breach of copyright.

User names and passwords must be kept private and staff, pupils and parents/carers should not try to access the site via other user's logons.

Access is restricted within the site for example, parents can only view their own children's classes and only the class teacher or administrator can update a class area.

If a user's behaviour on the VLE is deemed to be unacceptable the user will be removed or have their access restricted.

Procedure for using mobile phones and Personal Digital Assistants (PDAs)

In accordance with the Recommended Use Policy staff should not answers calls or texts when in the classroom or working with children. It is advised that mobile phones are switched off.

We strongly discourage children from bringing mobile phones to school as many phones now have cameras and internet access which we cannot monitor.

Children bringing mobile phones to school should hand the phone in to the office until the end of the school day.

Sanctions to be imposed if procedures are not followed

- Letters may be sent home to parents or carers
- Users may be suspended from using the school's equipment or access to the VLE reduced or removed for an appropriate period of time
- Details may be passed on to the police in more serious cases.
- Legal action may be taken in extreme circumstances.