



Whitley Abbey Primary School

E-Safety Policy

January 2018

To be reviewed January 2019

Preface

The purpose of Internet access at Whitley Abbey Primary School is to raise educational standards, to support the professional work of staff and to enhance the school's management information and business administration systems. Access to the Internet is a *necessary tool* for staff and is an *entitlement* for children.

In common with other media such as magazines, books and video, some material available via the Internet is unsuitable for pupils. The school will supervise pupils and take all reasonable precautions to ensure that users access only appropriate material. However, due to the international scale and linked nature of information available via the Internet, it is not possible to guarantee that unsuitable material will never appear on a computer. Neither the school nor Coventry LA can accept liability for the material accessed, or any consequences thereof.

No method of access control is fool proof.

The only method of providing a totally safe computer environment use is to turn off all computers and to disconnect all internet access.

As this is not a practical or realistic situation in the modern educational environment several methods of internet management are in place.

Internet Access Management

Internet access is controlled through several layers.

The difference between unsuitable and inappropriate.

Unsuitable websites.

These are sites that are unsuitable to the current needs of the user in an educational environment.

This could be a site that is too complicated or contains too much irrelevant information for the user to manage.

Some sites may be unsuitable in a teaching environment (lessons) but be perfectly OK at other times- for examples games sites in Golden Time or shopping sites after school.

Inappropriate websites.

These are sites that contain material that is deemed not suitable for viewing/reading in a primary school environment (for example pornography, racism, religious persecution etc.).

Caveat: A website is deemed inappropriate by the school. As such our view may not agree with the views of others (e.g. parents) whose views may differ on what is appropriate.

How we manage the internet.

There are three main levels of management, each is as important as the other and all work together to provide for our internet safety.

- Staff observing.
- Smoothwall Filtering.
- Impero Education Software.

Staff observing.

Observation and supervision by staff is important. During web searches or when linking to new sites/pages unsuitable material may be accessed. It is up to staff to be vigilant and supervise children when the internet is used.

Staff should note any inappropriate site visited and pass the information to the ICT Coordinator for further action.

Smoothwall Filtering.

This system filters sites based on a list that is regularly reviewed and updated by our internet service provider- Smoothwall .

This is a 'global' systems that manages many LA schools and as such denies access to sites that may be deemed OK by some schools but not others.

Impero Education Software

This system works on two levels.

It controls access to sites based on their content (words or pictures) or those on a list.

It also allows the manager to review what websites have been visited, when and by whom.

This tracking is manageable by the school and will be reviewed on a regular basis. The Head of school will manage staff access records and the ICT Coordinator will manage the pupil access records.

Internet access infringement.

Staff Access will be managed by the Headteacher and any access deemed as unsuitable or inappropriate will be dealt with accordingly by him/her in accordance with school staff management procedures.

Pupils Access will be managed by the ICT Coordinator.

Any pupils seen to be accessing or trying to access inappropriate sites should be dealt with in the following manner as soon as possible after the event.

1. Pupil name to be passed to ICT Coordinator for tracking purposes using Forensic software.
2. Sites accessed to be noted by staff member (if possible) and /or the computer used to be noted (for tracking and management purposes).
3. Phase Leader staff to be informed.
4. Headteacher to be informed. He/She will decide if further action is required.
5. If site is deemed inappropriate then it will be passed to Redstone as request for filtering and added to the Forensic software for filtering.

Keeping Children Safe Online

E-safety will be a core focus of the computing curriculum and an aspect of this will be covered in every computing lesson, cross curricular opportunities will also be taken. This will include work through PSHE lesson to include social media and cyber-bullying. CEOP materials will be used in lessons, during assemblies and to inform parents.

Prevent duty

Children are taught how to keep safe on line, in line with the Prevent Duty (as detailed in the Child Protection Policy).

Contact with Parents

If school knows that children are putting themselves in danger online, whilst accessing the internet outside of school, we will liaise with parents to offer support and advice on how to keep their child safe. When issues arise in the school or in particular year groups, further information and advice about the issue may be sent home to the whole year group e.g. use of Youtube, online gaming/

Questions to consider:

Was the access accidental? If so how (sites search, link for another site etc).

Was this a deliberate access (Site address brought in from home for example)?

Has this pupil done this before?

What was the content of the site? (To help deem suitability.)

Signed Chair or Governors

Headteacher