What is E-Safety?

Whilst the internet and associated technologies are an excellent tool and resource to enrich learning there are still dangers related to their use, especially in relation to young students.

Some examples of these are:

• Bullying via chat or email

• Obsessive internet use

• Exposure to inappropriate materials

• Inappropriate or illegal behaviour

• Physical danger of sexual abuse

As a school it is our duty of care alongside that of parents and other members of the community to protect our children from these dangers and this can be achieved by many different mechanisms working together. The purpose of this e-safety policy is to outline what measures West End School takes to ensure that children can work in an e-safe environment and that any e-safety issue is detected and dealt with in a timely and appropriate fashion.

General policy statement

The School will endeavour to ensure the e-safety of all personnel (including children). It will use education, technology, accountability, responsibility and legislation as the key ways to achieve this.

Whole School responsibilities for e-safety

Within the school all members of staff and children are responsible for e-safety, responsibilities for each group include:

Children

• Participating in and gaining an understanding of e-safety issues and the safe responses from e-safety training sessions.

• Compliance with a highly visible student's Acceptable Use Policy (AUP) which children must agree to each time they use school ICT equipment either in the school or remotely which connects to the internet.

• Reporting any e-safety issue to the teacher, team leader or parent.

• Take responsibility for their own actions using the internet and communications technologies.

All Staff

• Have a clear understanding of e-safety issues and the required actions from e-safety training sessions.

• Reporting any e-safety issues to the ICT subject leader as soon as the issue is detected.

• Compliance with a highly visible staff Acceptable Use Policy (AUP) which staff must agree to each time they use school ICT equipment either in the school or remotely which connects to the internet.

Teaching Staff

• Educating children about e-safety through specific e-safety training sessions and reinforcing this training in the day to day use of ICT in the classroom

Network Manager (at present Edit Solutions)

• Deals with e-safety breaches from reporting through to resolution in conjunction with the ICT support team.

• Works with the ICT subject Leader to create, review and advise on e-safety and acceptable use policies.

• Works with outside agencies including the police where appropriate.

• Maintains a log of all e-safety issues.

How the school ensures e-safety in the classroom

Educating children in e-safety

A clear objective of the school is to educate children in safe use of ICT and the internet. We feel this is one of the best ways to minimise the potential for any e-safety issues to occur.

• Children will receive specific e-safety lessons aimed at ensuring that:

• Children know the e-safety risks that exists and how to identify when they are at risk.

• Children know how to mitigate against e-safety risks by using e-safe practices whilst online.

• Children know when, how and to whom to report instances when their e-safety may have been compromised.

• Children know that they are in an environment that encourages them to report e-safety issues without risk of reprimand, humiliation or embarrassment.

In addition to this specific training all members of staff will have a duty to reinforce e-safety practices wherever possible and will offer students advice and support in the classroom where minor e-safety incidents have occurred.

E-Safety education information will have high visibility in all areas of the school

How technology is used

The school will employ many different technologies to help to ensure e-safety for all the school members;

• The school will use internet filtering to block inappropriate content and in addition block websites which are irrelevant to the student's programme of study and are considered time wasting.

• The school will use a system which tracks all student activity on the school's computers. This system will automatically flag potential e-safety issues which will be monitored and then can be investigated by the support for learning team.

• The school will restrict which activities the children can perform using ICT and the internet through systems security policy and access control.

• Teaching staff will use control mechanisms to attempt to limit the applications and web sites which the children can visit whilst using ICT within a lesson.

How the School will respond to issues of misuse

The following are provided for the purpose of example only. Whenever a child or staff member infringes the e-Safety Policy, the final decision on the level of sanction will be at the discretion of the Head Teacher

Children

- Unauthorised use of mobile phone (or other new technologies) in lessons e.g. to send texts to friends
- Use of unauthorised instant messaging / social networking sites
- Accidentally accessing offensive material and not notifying a member of staff of it
- Deliberately corrupting or destroying someone's data, violating privacy of others
- Sending an email that is regarded as harassment or of a bullying nature
- Deliberately trying to access offensive or pornographic material
- Deliberately accessing, downloading and disseminating any material deemed offensive, obscene, defamatory, racist, homophobic or violent
- Receipt or transmission of material that infringes the copyright of another person or infringes the conditions of the Data Protection Act, revised 1988
- Bringing the school name into disrepute

Staff

• Excessive use of Internet for personal activities not related to professional development e.g. online shopping, personal email, instant messaging etc.

- Misuse of first level data security, e.g. wrongful use of passwords
- Breaching copyright or license e.g. installing unlicensed software on network
- Deliberately accessing, downloading and disseminating any material deemed offensive, obscene, defamatory, racist, homophobic or violent;
- Receipt or transmission of material that infringes the copyright of another person or infringes the conditions of the Data Protection Act, revised 1988;
- Any deliberate attempt to breach data protection or computer security rules;

- Bringing the School into disrepute.

Possible Sanctions (for both staff and children)

Referred to Headteacher /exclusion / removal of equipment / referral to police / LA e-safety officer

Working with parents and the community

Clearly many school children will also have access to ICT and the internet at home, often without some of the safeguards that are present within the school environment. Therefore parents must often be extra vigilant about their child's e-safety at home. One of the goals of the school is to support parent's role in providing an e-safe environment for their children to work in outside the school. The school will do this in several ways;

- Publish e-safety information and direct parents to external e-safety advisories via the school website
- Use external agencies to support children in staying safe in the e safety environment.

.