Westbourne Primary School E- Safety Policy

For Children

-E-safety will be embedded in the taught curriculum through discrete ICT lessons and ICT being taught across the curriculum.

Safety on the internet i.e. social networking/ safeguarding personal information

How to deal with inappropriate content on the internet.

Issues around copyright and using images/ sounds from other places.

Dangers of obsessive use and how to spot obsessive use

The importance of password protection and security.

Dangers of SPAM e-mails and how to deal with them safely

The concept that the internet is a forum for views and opinions not fact. Information on the internet should always be challenged and questioned.

-ICT at Westbourne Primary School will embrace the culture of password protection. Each child will have a user-id. This will be first name/second initial i.e. jbloggs. Each user id will be password protected. Passwords will be year group name and then a letter or number i.e. year6a. Children will be taught the importance of password protection throughout school as signposted by the ICT scheme of work. Any incidents of children sharing or misusing passwords will be dealt with by children having user ids and access to computers temporarily suspended. Children will have the same user id and password to log into the school website and for school email.

-Images of children will be displayed on the school website. Parents of children will be given the opportunity to opt out by returning an annual letter. This letter will be accompanied by an e-agreement form. This form will outline expectations for appropriate use and dangers of the internet. This form will be completed annually.

-A specific and simple protocol for both pupils and staff to log incidents of breaches of e-safety will be put into place. The recording and logging of incidents of any:

a) inappropriate images b) cyber bullying (signpost to 'cyber bullying' policy)

c) inappropriate use of other technology in school

(Link to child protection policy/ any serious incidents will be reported to the named person and recorded in the e-safety incident book). Children will be taught how to report finding an offensive website immediately. This will be reported to class teacher or supervising adult who will then report it to the e-safety officer.

-Children SHOULD NOT have unsupervised access to ICT equipment in school, including computers.

-Children are NOT ALLOWED to bring personal devices into school. This includes mobile phones, cameras, video recorders, USB sticks etc. Any that are found will be with held until an adult collects the child.

-Children will be taught appropriate use of e-mail at appropriate points throughout school. This will be signposted by the ICT scheme of work. Children will all have access to a school email solution. This will be password and user id protected. Children will be expected to use this email service appropriately. Any incidents of misuse will

be dealt with by suspension of their email account and possibly other forms of ICT for an agreed time. (signpost to cyber-bullying policy).

For Staff

-E-safety will be embedded in the taught curriculum through discrete ICT lessons and ICT being taught across the curriculum. E-safety is clearly highlighted in the ICT scheme of work. Teaching staff have a duty to teach each of the following:

Safety on the internet i.e. social networking/ safeguarding personal information

How to deal with inappropriate content on the internet.

Issues around copyright and using images/ sounds from other places.

Dangers of obsessive use and how to spot obsessive use

The importance of password protection and security.

Dangers of SPAM e-mails and how to deal with them safely

The concept that the internet is a forum for views and opinions not fact. Information on the internet should always be challenged and questioned.

(Refer to the medium term ICT scheme of work for more details)

-Each permanent member of staff (and in some cases long term temporary members of staff) will have a userid and password to log on to the school network. These passwords should not be shared with anybody else. Any visitor requiring access to the school network should be directed to the school office for a guest userid and password. These guest userids will be changed after use.

-Mobile phones are permitted in the staffroom and PPA room. Mobile phones should not be used in any other part of school (The ICT technician and the site manager are exempt from this rule). If a member of staff needs to make an urgent call during this time they must use a school phone or return to the staffroom. If an urgent call needs to be made to a member of staff during this time the call must be made to the main school number. Any exceptions to this rule must be passed by the Head Teacher.

-Mobile phones are permitted in the SSA as long as they are used in case of an emergency. Mobile phones must be taken to the SSA in cases of staff working there alone.

- Personal devices such as cameras and video recorders (and mobile phone cameras on school trips) are permitted as long as the images are downloaded immediately and NOT taken out of school. If children take images of staff they must be downloaded immediately and NOT taken out of school.

-School equipment (i.e. desktop computers and teacher laptops) must be used for school matters only (planning, school based research, etc). Teacher laptops are permitted to be used at home by the owner but again, must only be used for school related work.

- Social networking, personal ticket booking and personal shopping websites are not permitted in school or on school equipment (including teacher laptops at home or in school). Members of staff who do use social networking sites MUST NOT discuss any matter involving school life. It is NOT good practice to allow pupils or ex pupils access to your social network site. Any attempts by pupils to gain access should be logged and reported to the e-safety officer. Serious cases of misconduct have been highlighted in some schools and serious disciplinary action has had to be taken.

-Any request to unblock a fire walled website must be cleared by the e-safety officer and good reasons relating to improving learning and teaching must be given.

-The security of the school network and how this deals with e-safety issues is the responsibility of both the ICT leader and the ICT technician. Any problems or issues with the security of the school system must be reported to the e-safety officer.

For Stakeholders

-Stakeholders are signposted to the e-safety part of the school website. Sufficient and relevant e-safety is available here. This is particularly aimed at parents of children in school and deals with:

Leaving children alone with computers

Installing and sustaining effective firewalls on home PCs

The dangers of obsessive behaviour with computers and the internet

Having an awareness of what your child is doing on their computer

The dangers of cyber-bullying

- Stakeholders are asked to adhere to the no-mobile phone policy in school. Mobile phones must be turned off in school and visitors are asked not to use their mobile phones in school.

- Visitors to school ARE NOT permitted to take images (either camera or video) of children on school premises. This will be made clear in letters to stakeholders about specific school events (i.e. sports day, performances). Any incidents will be reported to the e-safety officer.

-Certain stakeholders (governors/ supply teachers) must make themselves familiar with staff guidance on e-safety and the acceptable use policy and adhere to the appropriate guidance where applicable.

Linked policies

Behaviour and anti bullying policy

This policy will be reviewed and updated within the ongoing cycle of policy review implemented by the school.

Date established by Governing Body:

Date for full implementation:

Date for review:

Acceptable Use Agreement (AUA) for Staff

I agree that:

I will read and keep reminding myself of the school e safety policy. I will act to support and promote it with other staff, pupils and stakeholders.

I agree that any use of school ICT systems and equipment will be for professional purposes as agreed by the school.

I agree that any online activity will not harass, harm, offend or insult other users. Any activity will not intentionally cause offence, harass, insult anyone involved with the school or not.

I agree to keep my usernames, passwords and other logon details secure and will not reveal or share them. Care will be taken to ensure I logout when not actively using the school system.

I will not allow an unauthorised person to access the school ICT systems, e.g. by logging in for them. I will direct them to the office for a guest username.

I will take care of my school laptop and understand that this is to be used for school affairs only. (See attached appendix for school laptops). I agree to pay any excess charge (up to £100) to cover the repair of any damage caused by my own negligence.

I will not search for, download, upload or forward any content that is illegal, or that could be considered offensive by another user on school equipment. If I accidentally encounter such material I will follow the school's procedure and report this immediately. (See e-safety policy)

I will not access personal social networking sites, personal ticket booking sites or personal shopping websites in school or on school devices. I understand that this is in accordance with the school's safety policy.

I will not download or install any hardware or software on school equipment. I will follow the procedure for requesting new hardware or software. (see e safety policy)

I will act to ensure that any files that come from a source outside school are free from viruses and other malware before using them on any school equipment.

I will not hold sensitive data such as details of pupils, parents or other stakeholders without specific permission from the Head Teacher. Any sensitive data will only be held in password protected or otherwise encrypted folders or files.

Any communication in school or on school equipment will be through school e-mail or through other school systems e.g. learning platforms, and should relate to school matters only.

I understand that it is not acceptable to contact pupils using personal equipment or personal contact details, including my own mobile phone or through my personal social network profiles. (See e-safety policy)

I will not give out my personal details, or the personal details of other users, to pupils or parents or on the Internet. I will ensure my home address, personal telephone numbers and personal email accounts are not shared with children or parents. I understand that my school email details can be shared but will be used solely for the purpose of teaching and learning.

I will ensure that any activity, including messages sent and posts made on websites, and including activity outside of school, will not bring my professional role or the name of the school into disrepute.

Personal devices such as cameras and video recorders (and mobile phone cameras on school trips) are permitted as long as the images are downloaded immediately and NOT taken out of school. I will take all reasonable steps to make sure that if children take images of me they must be downloaded immediately and not taken out of school.

I understand that my mobile phones will only be used in the staffroom and PPA room (except for people working alone in the SSA building where mobiles can be switched on for safety and security).

I understand that the I.C.T. technician and some other visitors are allowed to use their mobile phone inside the 'no mobile phone area' but only on occasion where it is such communication is essential for them to perform their job effectively.

Finally:
I understand that the files used or stored on school equipment, including any communication and other internet activity may be monitored and that action may be taken if this is deemed necessary to safeguard myself or others.

I agree that the statements in this AUA are to ensure my own professional protection.

I understand that if I do not follow all statements in this AUP and in other school policies I may be subject to disciplinary action in line with the school's established disciplinary procedures.

Name_____ Signed_____
Date_____

AUA Teacher Laptop Appendix

I agree that the statements in this AUA and AUA laptop appendix are to ensure my own professional protection.

I understand that this is a school laptop and will be used solely for school work and school matters.

I will take all reasonable measures to ensure that my laptop is safe and secure at all times.

I have read and agree to adhere to the statements in the AUA in relation to my school laptop.

I will inform the ICT technician about any problem with my laptop as soon as possible and understand that he/she will make every effort to correct the problem.

I will bring my laptop to school everyday and use it to aid teaching and learning by running the interactive whiteboard. If I can not guarantee to bring it the following school day I will leave locked and secure in school overnight.

I will ensure that pupils will not use my school laptop unless directly supervised and using the interactive whiteboard.

I will not access personal email or social networking sites on my school laptop. School email will be used for any email correspondence connected to my professional role. The school learning platform will be used for professional networking.

I understand that internet browsing on my school laptop is appropriate when used to access resources to support learning and teaching.

I understand that any files stored on my school laptop including any communication and other internet activity may be monitored. This includes when I use my school laptop at home.

I understand that if I do not follow all statements in this AUA appendix that I may be asked to explain my actions which may lead to disciplinary action in line with the schools established disciplinary procedures.

Signed:

Date: