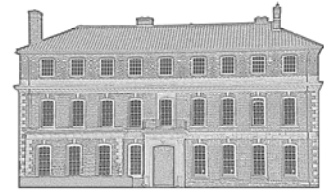


# WINDLESHAM HOUSE SCHOOL



## E SAFETY POLICY

**Reviewed: January 2011**

**Policy Ref: 036**

**Windlesham**

### 1) Policy Statement – ICT At Windlesham

- a) ICT at Windlesham is an integral part of day to day life for both the Children and the staff. E-Safety is at the forefront of all the systems in place at school and is an ever involving process with the onset of emerging technologies. We do not teach ICT as a subject but use it constantly in the classroom environment and therefore expect our staff to be fully abreast of the benefits and dangers involved with the use of internet based technologies and to promote appropriate, effective and safe use within their teaching.
- b) There are measures in place at Windlesham to keep the children safe whilst using these technologies at school. We aim though to educate children to enable them that they do not get themselves in dangerous situations whilst using the internet at home or in other situations, using mobile or other handheld devices.

This policy also applies to our Early Years Foundation Stage and after School care.

### 2) The role of the Staff at Windlesham whilst using and Teaching with ICT

- a) Internet Safety is a whole school responsibility and the staff must be ever mindful of this in their teaching and their personal use of ICT within the school.
- b) We need to teach children to use the internet and ICT safely, responsibly and respectfully. We need to teach children to view the internet with a critical eye, that not everything they read is true.
- c) It is essential that the staff are aware of the School Network Rules and to ensure that children are using the computers in school in accordance with these. It is however important that staff are aware of what children are using computers for outside of the relative safety of the school network.
- d) The school will ensure that the use of Internet derived materials by staff and pupils complies with copyright law.

### 3) Managing Access to Internet at School

- a) Internet access is filtered through the Navaho Server. All accesses to the internet including failed internet searches are logged both for children and for staff.
- b) There is no access to social networking sites, web-based mail (such as Hotmail) chatrooms, Online Games, MSN and uTube for children whilst they are in school. Staff are able to access these sites when in school, but not during the presence of children.
- c) Staff are asked to be always vigilant, in particular when children are using the internet in freetime. Children may use the internet for school work and approved activities (hobbies, sports sites etc) but may not play games, unless they are on the BBC site (and only after supper) ,may not use any sites designed for outside communication or any site which contains inappropriate content.
- d) If staff or pupils discover an unsuitable site, it must be reported to the Head of ICT.
- e) Our filtering solution will only allow children to use Google searching whilst using the Safe searching Facility. All uses not using this will be blocked out.

# WINDLESHAM HOUSE SCHOOL

## E SAFETY POLICY

f) Virus protection throughout the school is updated daily.

#### 4) Managing access to Email at School

- a) All Prep School children have their own Webmail account, which is also accessible from home via <http://mail.windlesham.com>. Children have no access to any other email accounts in school.
- b) Email is filtered for bad words, spam and any inappropriate content.
- c) Children do not have access to external web-based email accounts such as Hotmail, Googlemail etc.
- d) Staff have an Exchange email account which is accessible via the school network, remote access or via Smartphone (iphone or Blackberry). Staff are allowed to access their own personal emails via the school network.

<sup>1</sup> Children must be encouraged never to give out personal information, via email or with any email communication, though this will not be possible for them to do in school. Children will have access to do this at home and discouraged from doing this. Children should not agree to meet someone that they have made contact with via the internet\email.

<sup>2</sup> Everyone is reminded not to give any personal information out in emails – there are a huge amount of spam or Phishing emails, which are fraudulently trying to get hold of important personal and banking information – NEVER give out this information in an email.

- e) All mail is checked for virus when entering the school network and staff emails are checked a second time when entering the School Exchange Server. However carefully viruses are checked users are always encouraged not to open unknown emails or attachments.
- f) Chain mail – all Windlesham Email users both Staff and Children are asked not to fall for and to forward unnecessary emails. Do not send unnecessary emails to staff groups.
- g) Children must never send emails to other children in school – it can lead to problems and it is far better to talk directly to your friends.

#### 5) Managing Remote Access to the School Network

- a) Staff and Year 8 (1s) are able to fully access the school network at home via Remote Desktop Protocol (RDP)
- b) All users are asked to be vigilant and to log off after use particularly if using in a public location.

#### 6) Using the School Network Safely both Staff and Children

- a) All network users must use an appropriate password and always remember to log out after use. It is the responsibility of the user and it is critical that staff do not allow children access to their own personal account.
- b) We must encourage children to not give out personal details over the internet or via email in any situations and staff should be very mindful of what and whom they give out details to.
- c) Staff must ensure that the children are familiar with the School Network rules which are published next to each computer in school and in the pupil handbook. (Appendix 1)

# WINDLESHAM HOUSE SCHOOL

## E SAFETY POLICY

- d) Staff must be aware of the Acceptable Use Policy for Staff (Appendix 2) and must be signed by all new staff to the school.

### 7) **Publishing pupil's images and work**

All parents are contacted regarding permission to publish children's photographs in either our printed literature, in the press or the website

### 8) **Protecting personal data**

Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 1998

### 9) **Managing Emerging Technologies**

- a) Whilst we recognise and review the use of emerging technologies, we do not allow the use of mobile, handheld devices and music players with screens in school by children. Children in the 1s have the privilege of using an MP3 (available from the school shop) without a screen and may be used up in the dorms only.
- b) Publishing Children's Photographs on the Website
- c) Photographs that include pupils will be selected carefully and will not directly name any individual child.
- d) Written permission from parents is requested before allowing photographs of children to be published on the website or in publications.

### 10) **Managing Video-Conferencing at School**

- a) Due to limitations on Broadband access we have not used this technology widely, but on individual basis for parental contact via Skype and for one-to-one lessons. This is always carried out on a supervised basis, with the connection made by a member of staff.
- b) Computers in the main ICT rooms do not have access to Video Conferencing.

### 11) **Guidelines for Parents regarding Internet Security at Home**

- a) We also regularly issue the following guidelines to parents, to encourage safe use of internet technologies at home:
- b) The Internet, as we know is a fantastic resource full of rich informative sites and of course many fun and entertaining games, but there are also dangers and pitfalls.
- c) When the children are in school they are very much protected whilst using the internet. Having in place security which filters out the unpleasant sites and does not allow access to gaming, social networking and other sites which we consider unsuitable and unnecessary for children at Prep School, we can also monitor which sites children are visiting and those that they try to visit! This needs to be thought about carefully for when children are at home as often they have access to far more than they would at school. All of our children have PSHE sessions from our police liaison officer on the dangers and the pitfalls of the internet, but we ask that you consider the suggestions below:
- d) Always have your home Computers, Playstations, Xbox in central places in the home not shut away in bedrooms.

# WINDLESHAM HOUSE SCHOOL

## E SAFETY POLICY

- e) Think about filtering software to protect your home computer, eg [www.netnany.com](http://www.netnany.com).

Do not allow your children to sign up and give out personal information across the internet without your permission; see what type of sites your child is visiting and make use of the internet history which is available on all internet browsers. Discuss these with your children.

- f) Children are not allowed to sign up to social networking sites such as facebook until they are 13 years old. If your child has already signed up to this, unless they are already 13, they have already lied about their age!
- g) Ensure that you are familiar with the types of sites your child is visiting and that they are using appropriate privacy settings on profiles and they are not giving out personal information like home address, age, school, mobile phone number.
- h) Younger children are drawn to the games that are available online and sites like Club Penguin are hugely popular, but it does mean that in these games these children are communicating with others whom they do not know online. It is also worth considering whether children are playing excessively on these sites when they would be far better off reading or enjoying the fresh air playing outside.
- i) There is potential for children to become obsessed with the internet and related technologies, It is therefore essential that home use must be managed effectively by the parents.
- j) Make sure that your Google settings are set up for strict filtering.

### 12) Authorising Internet access

- a) All staff must read 'Acceptable ICT Use Agreement' before using any school ICT resource.
- b) 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.
- c) At Key Stage 1, access to the Internet will be by adult demonstration with occasional directly supervised access to specific, approved on-line materials.
- d) Parents and Children will be asked to sign and return a consent form (Appendix 3).

### 13) Assessing risks

- a) 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 can accept liability for the material accessed, or any consequences of Internet access.
- b) The school will audit ICT provision to establish if the e-safety policy is adequate and that its implementation is effective.

### 14) Handling e-safety complaints

- a) Complaints of Internet misuse will be dealt with by a senior member of staff. Any complaint about staff misuse must be referred to the Headmaster.
- b) Complaints of a child protection nature must be dealt with in accordance with school child protection procedures.
- c) Pupils and parents will be informed of the complaints procedure.

# **WINDLESHAM HOUSE SCHOOL**

## **E SAFETY POLICY**

- d)** Discussions will be held with the Police Liaison Office to establish procedures for handling potentially illegal issues.