The White House Preparatory School

Woodentops Kindergarten and Woodentops Day Nursery

PREP SCHOOL and EARLYYEARS

INTERNET USE & eSafety POLICY

Scope of this Policy

This policy applies to all members of the school community, including staff, pupils, parents, and visitors. In this policy 'staff' includes teaching and non-teaching staff, Principles and regular visitors (but access to systems is not intended in any way to imply an employment relationship). 'Parents' include, where applicable, pupils' carers and those with parental responsibility. 'Visitors' includes anyone else who comes to the school, including occasional volunteers.

Online behaviour

As a member of the school community you should follow these principles in all of your online activities:

- Ensure that your online communications, and any content you share online, are respectful of others and composed in a way you would wish to stand by.
- Do not access, create or share content that is illegal, deceptive, or likely to offend other members of the school community (for example, content that is obscene, or promotes violence, discrimination, or extremism, or raises safeguarding issues).
- Respect the privacy of others. Do not share photos, videos, contact details, or other information about members of the school community, even if the content is not shared publicly, without going through official channels and obtaining permission.
- Do not access or share material that infringes copyright, and do not claim the work of others as your own.
- Do not use the internet to distribute malicious software, to damage, interfere with, or gain unauthorised access to the computer systems of others, or carry out illegal activities.
- Staff should not use their personal email, or social media accounts to contact pupils or parents, and pupils and parents should not attempt to discover or contact the personal email addresses or social media accounts of staff.

Using the school's ICT systems

Whenever you use the school's ICT systems (including by connecting your own device to the network) you should follow these principles:

- Only access school ICT systems using your own username and password. Do not share your username or password with anyone else.
- Do not attempt to circumvent the content filters or other security measures installed on the school's ICT systems, and do not attempt to access parts of the system that you do not have permission to access.
- Do not attempt to install software on, or otherwise alter, school ICT systems.
- Do not use the school's ICT systems in a way that breaches the principles of online behaviour set out above.
- Remember that the school monitors use of the school's ICT systems, and that the school can view content accessed or sent via its systems.

Passwords

Passwords protect the School’s network and computer system and are your responsibility. They should not be obvious (for example "password", 123456, a family name or birthdays), and nor should they be the same as your widely-used personal passwords. You should not let anyone else know your password, nor keep a list of passwords where they may be accessed, and must change it immediately if it appears to be compromised. You should not attempt to gain unauthorised access to anyone else's computer or to confidential information to which you do not have access rights.

Use of Property
Any property belonging to the School should be treated with respect and care, and used only in accordance with any training and policies provided. You must report any faults or breakages without delay to the Headteacher.

Use of school systems
The provision of school email accounts, Wi-Fi and internet access is for official school business, administration and education. Staff and pupils should keep their personal, family and social lives separate from their school ICT use and limit as far as possible any personal use of these accounts. Again, please be aware of the school's right to monitor and access web history and email use.

Use of personal devices or accounts and working remotely

- All official school business must be conducted on school systems, and it is not permissible to use personal email accounts for school business.
- Any use of personal devices for school purposes, and any removal of personal data or confidential information from school systems – by any means including email, printing, file transfer, cloud or (encrypted) memory stick – must be registered and approved by the Headteacher.

Where permission is given for use of personal devices, these must be subject to appropriate safeguards in line with the school's policies.

Monitoring and access
Staff, parents and pupils should be aware that school email and internet usage (including through school Wi-Fi) will be monitored for safeguarding, conduct and performance purposes, and both web history and school email accounts may be accessed by the school where necessary for a lawful purpose – including serious conduct or welfare concerns, extremism and the protection of others.

As a rule pupils are not permitted to bring personal devices into school however should this happen, with or without permission, any personal devices used by pupils may be confiscated also examined if there is good cause to do so. The school may require staff to conduct searches of pupil's personal accounts or devices if they were used for school business in contravention of this policy.

Compliance with related school policies
You will ensure that you comply with the school's e-Safety Policy and any other relevant policies e.g. Retention of Records, Safeguarding, Bullying, Data Protection Policy.

Retention of digital data
Staff and pupils must be aware that all emails sent or received on school systems will be stored, archived or deleted according to our storage policy. Our storage policy is applied to email accounts and contents of a colleague leaving the school. Important information that is necessary to be kept should be held on the relevant personnel or pupil file, not kept in personal folders, archives or inboxes. Hence it is the responsibility of each account user to ensure that important information (or indeed any personal information that they wish to keep, in line with school policy on personal use) is retained in the right place or, where applicable, provided to the right colleague. That way no important information should ever be lost as a result of the school's email deletion protocol.

If you consider that reasons exist for the protocol not to apply, or need assistance in how to retain and appropriately archive data, please contact the Headteacher.

Breach reporting
The law requires the school to notify personal data breaches, if they are likely to cause harm, to the authorities and, in some cases, to those affected. A personal data breach is a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data.

This will include almost any loss of, or compromise to, personal data held by the school regardless of whether the personal data falls into a third party's hands. This would include:

- loss of an unencrypted laptop, USB stick or a physical file containing personal data;
- any external hacking of the school's systems, e.g. through the use of malware;
- application of the wrong privacy settings to online systems;
- misdirected post or email;
- failing to bcc recipients of a mass email; and
- unsecure disposal.

The school must generally report personal data breaches to the ICO without undue delay (i.e. within 72 hours), and certainly if it presents a risk to individuals. In addition, controllers must notify individuals affected if that risk is high. In any event, the school must keep a record of any personal data breaches, regardless of whether we need to notify the ICO.

If either staff or pupils become aware of a suspected breach they must report it to the Headteacher as soon as is possible and with in 24 hours of a breach being suspected.

Breaches of this policy
A deliberate breach of this policy will be dealt with as a disciplinary matter using the school's usual procedures. In addition, a deliberate breach may result in the school restricting your access to school ICT systems.

If you become aware of a breach of this policy or you are concerned that a member of the school community is being harassed or harmed online you should report it to Tony Lewis as the eSafety and Data Protection Officer. Reports will be treated in confidence.

See further below for rules to be used with KS1 and KS2 also wider eSafety rules.

Policy will be reviewed annually			
Policy reviewed:	Sept 16	By:	Headteacher
Policy reviewed:	Sept 17	By:	Headteacher
Policy reviewed:	Sept 18	By:	Headteacher
Policy reviewed:	Sept 19	By:	Headteacher
To be reviewed:	Sept 20	By:	Headteacher

Key Stage 1

Think then Click

These rules help us to stay safe on the Internet

We only use the internet when an adult is with us

We can click on the buttons or links when we know what they do.

We can search the Internet with an adult.

We always ask if we get lost on the Internet.

We can send and open emails together.

We can write polite and friendly emails to people that we know.

Key Stage 2

Think then Click

e-Safety Rules for Key Stage 2

- We ask permission before using the Internet.
- We only use websites that an adult has chosen.
- We tell an adult if we see anything with which we are uncomfortable.
- We immediately close any webpage we not sure about.
- We only e-mail people an adult has approved.
- We send e-mails that are polite and friendly.
- We never give out personal information or passwords.
- We never arrange to meet anyone we don’t know.
- We do not open e-mails sent by anyone we don’t know.
- We do not use Internet chat rooms.

e-Safety Rules for The White House Preparatory School and Woodentops Day Nursery

These e-Safety Rules help to protect pupils and the school by describing acceptable and unacceptable computer use.

- The information systems are school property and in certain circumstances it may be a criminal offence to use a computer for a purpose not permitted by its owner. As the school owns the computer network and can set rules for its use.
- Network access must be made via the user's authorised account and password, which must not be given to any other person.
- All network and Internet use must be appropriate to education and the users professional role.
- Irresponsible use may result in the loss of network or Internet access. This includes the installation of software or hardware with out permission and may be subject to disciplinary action.
- Copyright and intellectual property rights must be respected.
- Messages shall be written carefully and politely, particularly as email could be forwarded to unintended readers.
- Anonymous messages and chain letters are not permitted.
- System security must be respected at all times therefore aspects such as passwords or security information must never be revealed to anyone other than an appropriate system manager. Security is especially important when using or/and accessing remotely.
- Users must take care not to reveal personal information through email, personal publishing, blogs or messaging.
- The school ICT systems may not be used for private purposes, unless the head teacher has given specific permission. Use for personal financial gain, gambling, political activity, advertising or illegal purposes will never be permitted.
- The school may monitor all information systems and internet use to ensure policy compliance.
- All electronic communications with parents and pupils must be compatible with the employees professional role.
- All users will promote e-safety with pupils and, as appropriate, will help them to develop a responsible attitude to system use and to the content they access or create.
- All users must report any incidents of concern regarding children's safety to the school e-Safety Officer or the Designated Safeguard Lead, Tony Lewis.

The school may exercise its right to monitor the use of the school's computer systems, including access to web-sites, the interception of e-mail and the deletion of inappropriate materials where it believes unauthorised use of the school's computer system may be taking place, or the system may be being used for criminal purposes or for storing unauthorised or unlawful text, imagery or sound.

Internet use and E-Safety Audit

This quick self-audit will help the senior leadership team (SLT) assess whether the e-safety basics are in place.

Has the school an e-Safety Policy that complies with CYPD guidance?	**Y**
Date of latest update: **September 2019**	
The Policy is available for staff electronically and in hard copy	
And for parents on the School website and on request	
The Designated Safeguarding Lead is: **Tony Lewis**	
The e-Safety Officer is: **Tony Lewis**	
Has e-safety training been provided for both pupils and staff? ***Yes – through on-going INSET***	**Y**
Training providers are reviewed periodically including Lambeth provision, Think U Know, NSPCC etc	**Y**
The Internet Use and eSafety Policy is reviewed annually and all staff indicate their knowledge and understanding in the Annual Declaration. This is signed by any member of staff joining during the school year.	**Y**
Have school e-Safety Rules been set for pupils?	**Y**
Are children taught and reminded of rules involving ICT usage at school also re-enforce safer usage at home and outside of school.	**Y**
Internet access is provided by an approved educational Internet service provider.	**Y**
Has the school filtering policy has been approved by SLT?	**Y**
Is personal data collected, stored and used according to the principles of the GDPR?	**Y**

Appendix: Principles and Good Practice

eSafety

eSafety encompasses Internet technologies and electronic communications such as mobile phones and wireless technology. It highlights the need to educate children and young people about the benefits and risks of using new technology and provides safeguards and awareness for users to enable them to control their online experiences.

The school's Internet Use and eSafety policy will operate in conjunction with other policies including those for Pupil Behaviour, Bullying, Curriculum, Data Protection and Security.

Good Habits

eSafety depends on effective practice at a number of levels:

- Responsible ICT use by all staff and pupils; encouraged by education and made explicit through published policies.
- Sound implementation of e-safety policy in both administration and curriculum, including secure school network design and use.
- The appreciation of the Internet and eSafety Policy by all staff in their Annual Declaration
- Use of the school's Purple Mash ICT software and any other software which is made available as provision continues to develop.
- Education of pupils through eSafety timetabled on the ICT curriculum.

The school has appointed an e-Safety Officer who is the Designated Child Protection Officer as the roles overlap.

Why is Internet Use Important?

The purpose of Internet use in The White House School is to raise educational standards, to promote pupil achievement, to support the professional work of staff and to enhance the school's management information and administration systems.

Internet use is part of the statutory curriculum and a necessary tool for learning. It is an essential element in 21st century life for education, business and social interaction. Access to the Internet is therefore an entitlement for pupils who show a responsible and mature approach to its use. Our school has a duty to provide pupils with quality and appropriate internet access.

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

How does Internet Use Benefit Education?

Benefits of using the Internet in education include:

- access to world-wide educational resources including museums and art galleries;
- inclusion in the National Education Network which connects all UK schools;
- educational and cultural exchanges between pupils world-wide;
- access to experts in many fields for pupils and staff;
- professional development for staff through access to national developments, educational materials and effective curriculum practice;
- collaboration across support services and professional associations;
- improved access to technical support including remote management of networks and automatic system updates;

How can Internet Use Enhance Learning?

- The school Internet access will be designed expressly for pupil use and includes filtering appropriate to the age of pupils.
- All White House staff are trained on how to activate the Viglen Remote Learning Classlink system, which allows the teacher to control the pupils' internet access
- Pupils will be taught what Internet use is acceptable and what is not and given clear objectives for Internet use.
- Internet access will be planned to enrich and extend learning activities.
- Staff should guide pupils in on-line activities that will support learning outcomes planned for the pupils' age and maturity.
- Pupils will be educated in the effective use of the Internet in research, including the skills of knowledge location, retrieval and evaluation.

World Wide Web

- If staff or pupils discover unsuitable sites, the URL (address), time, content must be reported to the Deputy Headteacher, Headteacher or Principal.
- The White House School will ensure that the use of Internet derived materials by pupils and staff complies with copyright law.
- Pupils should be taught to be critically aware of the materials they are shown and how to validate information before accepting its accuracy.

Email

- The staff school email system is hosted by googlemail.
- The White House Preparatory School does not currently provide 'in-house' email facilities for our pupils.
- Pupils are not allowed to check any personal email accounts within the ICT suite and these sites can indeed be blocked by staff, thereby ensuring our PC's are not harmed by any external viruses.
- Users are responsible for all E-mails sent and for contacts made that may result in E-mails being received, professional conduct when sending emails using a school E-mail address is expected at all times.
- As E-mail can be forwarded or inadvertently be sent to the wrong person, the same professional levels of language and content should be applied as for letters or other media at all times;
- Posting anonymous messages and forwarding chain letters is forbidden;

Social Networking

- Social networking sites are to be blocked off by filtering software.
- At The White House Preparatory School access to social networking sites and newsgroups are currently available but controlled by the teacher's use of the Viglen remote learning system.
- Pupils, though advised on the good or better use of social networking sites and advised never to give out personal details of any kind which may identify them or their location
- Pupils are advised not to place personal photos on any social network space and shown how "posting" or "messaging" can lead to the loss of control of information especially that which they guard as being personal and private.

Internet Filtering

The school filters undesired material through a DNS Filter Network System. The on-going success is reviewed regularly by the ICT safety coordinator.

Go Guardian
GoGuardian Admin applies content filtering based on category, URL or real time analysis of content on the page. GoGuardian Admin is active on any Chromebook on which a pupils logs in using their school given GSuite credentials also on all devices used by staff accessing the internet via the school wifi. Subject to review settings can be changed by access to the GoGuardian Help Centre (here is a link to our Help Center.

Managing Emerging Technologies

- Emerging technologies will be examined for educational benefit and a risk assessment will be carried out before use in The White House Preparatory school and Woodentops Kindergarten and Day Nursery is allowed.

BYO Devices

- Pupils are not allowed to bring mobiles or other devices to school. The exception are those children who, by agreement with their parents, walk to and/or from school by themselves – usually Year 6 but occasionally Year 5 in preparation for transition to senior school. All use of mobile phones by pupils whilst at school is not permitted. The School does take an interest in usage outside of school and will respond if this impacts on children.
- Staff are not allowed to use their mobile phones either in class, or whilst walking around the school or Day Nursery buildings. Mobiles must be stored securely and away from children. Designated areas of usage include the Staff Room, the Head’s Office and the School Office.
- It is recognised staff may have downloaded the google/gmail app onto their mobiles and may choose to access emails and other aspects of the school system in that manner. They must ensure this is entirely secure and must be extremely discrete in accessing this whilst in public places.
- Staff who BYO tablet and/or laptop must register this with the Headteacher who will review the situation and conduct a risk assessment appropriate to the context.
- The sending of abusive or inappropriate messages in any form is forbidden.

Published Content and the School Web Site

- The contact details on the Web site should be the school address, e-mail and telephone number. Staff or pupils personal information will not be published.
- The Principal will take overall editorial responsibility and ensure that content is accurate and appropriate.

Electronic Publication of Pupils’ Images and Work

Currently the school website contains a limited range of photos and images and that is intentional. These may change from time to time and the following protocols are applied:

- Photographs that include pupils will be selected carefully and will not enable individual pupils to be clearly identified.

- Pupils' full names will not be used anywhere on the Web site or Blog, particularly in association with photographs.
- Written permission from parents or carers will be obtained before photographs of pupils are published on the school Web site.
- Work on the website can only be published with the permission of the pupil and parents.

Information System Security and Virus Protection

- School ICT systems capacity and security will be reviewed regularly.
- Virus protection is installed and is updated regularly.
- Staff laptops and PC's in the main building of the school are protected by 'Microsoft Security Essentials', set to run a virus scan once weekly. This scan is regularly reviewed by the ICT coordinator.
- Newer computers have Norton Anti-Virus installed on them.

Protecting Personal Data

Personal data will be recorded, processed, transferred and made available according to the GDPR 2018.

Assessing Risks - on-going

- The school will take all reasonable precautions to prevent access to inappropriate material. However, due to the international scale and linked internet content, it is not possible to guarantee that unsuitable material will never appear on a school computer. No internet content filtering system is 100% secure due to the ever changing nature of undesirable sites, virus or material.
- The school should audit ICT use to establish if the e-safety policy is adequate and that the implementation of the e-safety policy is appropriate.

Handling e-safety Complaints

- Complaints of Internet misuse will be dealt with by a senior member of staff most usually the eSafety Office and DSL, Tony Lewis.
- Any complaint about staff misuse must be referred to the Headteacher or Deputy Headteacher.
- Complaints of a safeguarding or/and child protection nature must be dealt with in accordance with school safeguarding and child protection procedures.
- Pupils and parents will be informed of the complaints procedure.