THE WHITE HOUSE PREPARATORY SCHOOL

The White House Preparatory School

Woodentops Kindergarten and Woodentops Day Nursery

PREP SCHOOL and EARLYYEARS

ICT Usage & eSafety Policy

This policy applies to all members of the school community, including staff, pupils, parents, and visitors. In this policy 'staff' includes Principals, teaching and non-teaching staff and peripatetic teachers. Reference to parents and visitors is included as appropriate to the circumstance.

Nb 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.

*This policy has been revised after just one year (rather than usual 2) to reflect KCSIE 2023 and responsibilities for filtering and monitoring. This has always been the practice of the school and the eSafety officer and further detail is now provided.

Principal Mrs M. McCahery Cert Ed **Headmaster** Joe Knight BA Hons, PCGE, NPQH
24 Thornton Road, London, SW12 0LF
020 8674 9514 office@whitehouseschool.com
www.whitehouseschool.com

THE WHITE HOUSE
PREPARATORY SCHOOL

Principles and Good Practice

ICT usage refers to the use of all devices whether owned by the school or personal devices, regardless of whether linked to the wifi, internet or not. ICT usage demands respect and responsibility at all times.

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 prime focus is access via the @whitehouseschool.com community whether on school site or off site. It applies to staff as well as pupils.

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 also Staff Code of Conduct and Behaviour.

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 eSafety 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 in the ICT curriculum.

THE WHITE HOUSE PREPARATORY SCHOOL

The eSafety Officer is also the Designated Safeguarding Lead (as the roles overlap) and currently this is Tony Lewis (Headmaster).

eSafety Rules for The White House Preparatory School and Woodentops Day Nursery

These eSafety 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 without permission and may be subject to disciplinary action.
- Copyright and intellectual property rights must be respected.
- Messages must 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. This relates to use of the school system and also all other systems to which staff and pupils may access.

See Appendix 1 for child focused specific guidance by key stage.

For Staff specifically:

- The school ICT systems may not be used for private purposes, unless the Headteacher has given specific permission. Use for personal financial gain, gambling, political activity, advertising or illegal purposes will never be permitted.
- The school will monitor all information systems and internet use to ensure policy compliance.
- All electronic communications with parents and pupils must be compatible with the professional role of teachers and as employees of the school where the school holds the highest standards.
- All users will promote eSafety 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 eSafety Officer and the Designated Safeguard Lead, Tony Lewis.

Online behaviour

All member of the school community must follow these principles in all online activities:

- Ensure online communications, and any content shared online, are respectful of others.
- 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 must 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. For staff who are parents of pupils separate protocols will be advised.

Responsibilities

It is the responsibility of every member of the school community to protect the integrity of the school system and to act so personal information is stored only on anything approved school devices and systems. USBs and other personal storage devices can be used for curriculum, teaching and learning purposes and must never be used to store personal information relating to any pupil, parent or colleague.

The school exercises its right to monitor the use of the school's computer systems. This may include accessing websites used, interception of e-mail and the deletion of inappropriate materials where it believes inappropriate or/and 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.

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.

THE WHITE HOUSE PREPARATORY SCHOOL

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 be blocked by staff, thereby ensuring our Laptops/Chromebooks are not harmed by any external viruses.
- Users are responsible for all emails sent and for contacts made that may result in emails being received, professional conduct when sending emails using a school email address is expected at all times.
- As email 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

- At The White House Preparatory School access to social networking sites and newsgroups are currently available but controlled via the school filter with controls set by the eSafety officer. In the main social networking sites are blocked and made accessible only as appropriate and on request.
- Pupils are advised on the good or better use of social networking sites and to never to give out personal details of any kind which may identify them or their location. Where possible they are advised of Apps which may involve location identification provision.
- 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.

THE WHITE HOUSE PREPARATORY SCHOOL

Using the school's ICT systems
When using the school's ICT systems (including by connecting your own device to the network) the following principles should be followed:

- Access to the school ICT systems is by use of discrete and individual username and password. These must never be shared.
- Security measures and privileges are in place for good reason. No attempt must be made to circumvent the content filters or other security measures installed on the school's ICT systems, nor to attempt to access parts of the system for which permission or privilege has not been permitted.
- 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.
- The school monitors use of the school's ICT systems, and the school can view content accessed or sent via its systems.

Passwords
Passwords protect the School's network and computer system. Personal and individual access details are the responsibility of each and every member of the school community. They should not be obvious (for example "password", 123456, a family name or birthdays), and nor should they be the same as other widely-used personal passwords. Passwords should not be shared, nor a list of passwords where they may be accessed, and must be changed immediately if it appears to be compromised. The School ICT Officer must be advised immediately. Tony Lewis and Laura Randall have admin access to the school system and can change emails and intervene to restore the integrity of the school system.

No member of the school community should attempt to gain unauthorised access to anyone else's computer or to confidential information to which they 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 Google Education Suite system, 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.

BYO Devices
Pupils: are not allowed to bring mobiles or other devices to school.
Exceptions:

- 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.

- If use of a Kindle, laptop or similar is likely to have a significant impact on a child's learning and development. The school may enter into individual agreements with appropriate protocols applied (e.g. daily search of content to ensure material on the device is age appropriate).
- Occasional curriculum related activity by permission in advance e.g. Year 6 mobiles phones for photography and artwork.

Any exception must be agreed in advance by the Head or Principals.

Parents and pupils should recognise that any personal devices used by pupils may be examined to ensure they contain age appropriate material. Devices will be confiscated if they contain inappropriate material or/and are used in an inappropriate manner and especially in breach of this policy. The school may require staff to conduct searches of pupil's personal accounts or devices if they were used in a manner related to the school and in contravention of this policy.

Staff: It is accepted that staff will have personal mobile phones. In addition some may use personal laptops or/and tablets.

- Staff are not allowed to use their mobile phones 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.
- Staff use of personal devices such as tablets and laptops may be permitted according to situation but only by permission in advance e.g. Drama/Dance/Ballet use of device to provide musical backing.
- Staff may download the google/gmail app onto their devices 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.

Visitors: Occasionally speakers and workshop providers will wish/need to use their own devices in line with their presentations. This will be actioned independently of the school wifi/internet provision. A guest access has been created but will be used only on a school device so all aspects of security apply. Guests are encouraged to bring their own storage devices which will be connected to a school device.

Parents: Parents will not be provided with access to the school wifi/internet provision.

Published Content and the School Web Site

- The contact details on the Website 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

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 Website 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 Website.
- Work on the website can only be published with the permission of the pupil and parents.

Filtering and Monitoring

Monitoring and access
Staff, parents and pupils should be aware the school system belongs to the school, that school email and internet usage (including through school Wi-Fi) will be monitored for safeguarding, conduct and performance purposes, for which 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.

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 all devices when connected to the school system/Google Education suite whether by on site wifi or remotely. Pupils use their @whitehouseschool.com credentials to log in to school devices such as Chromebooks and internet access is via the school wifi therefore GoGuardian is actively monitoring and filtering at all times. This remains the case when pupils log in remotely to the school system. The same applies to all staff using the school system whether on site through the school wifi or remotely.

GoGuardian sends email alerts to the School eSafety Officer, Tony Lewis, also to Vice Principal Laura Randall. These are reviewed as soon as they are registered.

- In the main the school filters are extremely sensitive and indicate very clearly the material is a very low level of concern and most usually has been accessed accidentally.
- Whether in school time, out of school time or in holidays, if an alert is picked up by TL or LM they will review appropriate action which may include immediate contact with parents if they assess that level of need. Otherwise the situation will be managed on return to school.
- The eSafety Officer works with the teacher responsible for that class at that time also with the class teacher to review if further action is required, this may reflect pastoral concerns for the pupil. Any consequent action, whether involving pastoral support, contact with the parent or disciplinary action are determined as soon as possible. The school reserves the right to respond in the best manner for each particular circumstance.

In addition to alerts, the eSafety Officer monitors GoGuardian regularly.

Information System Security and Virus Protection

- School ICT systems capacity and security will be reviewed regularly.
- Virus protection is installed and is regularly reviewed, also updated as appropriate.
- Staff laptops are protected by McAfee and Microsoft Fortress. Regular scans are set to take place.

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 audits ICT usage to review the effect of this ICT usage and eSafety policy is fit for purpose, changes to practice and policy are made in the light of these reviews.

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.

Compliance with related school policies

Everyone must ensure that they 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 a colleague considers that reasons exist for the protocol not to apply, or need assistance in how to retain and appropriately archive data, then they must contact the Headteacher.

Breach reporting

The law requires the school to notify personal data breaches (to the ICO under GDPR 2018), 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 of electronic material.

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 latest within 24 hours of a breach being suspected.

THE WHITE HOUSE PREPARATORY SCHOOL

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.

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
Policy reviewed:	Sept 20	By:	Headteacher
Policy reviewed:	Sept 21	By:	Headteacher

Principal Mrs M. McCahery Cert Ed **Headmaster** Joe Knight BA Hons, PCGE, NPQH
24 Thornton Road, London, SW12 0LF
020 8674 9514 office@whitehouseschool.com
www.whitehouseschool.com

THE WHITE HOUSE PREPARATORY SCHOOL

Policy reviewed:	Sept 22	By:	Headteacher
Policy reviewed:	Sept 23	By:	Headteacher
To be reviewed:	Sept 25	By:	Headteacher

Appendix 1: Key messages for pupils

Reception and EYs

This is how we stay safe when we use computers:

- I will ask a teacher or suitable adult if I want to use the computers/tablets
- I will only use activities that a teacher or suitable adult has told or allowed me to use
- I will take care of computers/tablets and other equipment

THE WHITE HOUSE
PREPARATORY SCHOOL

- I will ask for help from a teacher or suitable adult if I am not sure what to do or if I think I have done something wrong
- I will tell a teacher or suitable adult if I see something that upsets me on the screen
- I know that if I break the rules I might not be allowed to use a computer/tablet

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

Principal Mrs M. McCahery Cert Ed **Headmaster** Joe Knight BA Hons, PCGE, NPQH
24 Thornton Road, London, SW12 0LF
020 8674 9514 office@whitehouseschool.com
www.whitehouseschool.com

THE WHITE HOUSE
PREPARATORY SCHOOL

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

- We ask permission before using the Internet.
- We only use websites 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.

Principal Mrs M. McCahery Cert Ed **Headmaster** Joe Knight BA Hons, PCGE, NPQH
24 Thornton Road, London, SW12 0LF
020 8674 9514 office@whitehouseschool.com
www.whitehouseschool.com

THE WHITE HOUSE PREPARATORY SCHOOL

- 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.

Appendix 2: Internet use and E-Safety Audit in brief

Has the school an e-Safety Policy that complies with CYPD guidance?	**Y**
Date of latest update: **September 2022**	
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?	**Y**

Principal Mrs M. McCahery Cert Ed **Headmaster** Joe Knight BA Hons, PCGE, NPQH
24 Thornton Road, London, SW12 0LF
020 8674 9514 office@whitehouseschool.com
www.whitehouseschool.com

THE WHITE HOUSE PREPARATORY SCHOOL

Yes – through on-going INSET	
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 been approved by SLT?	**Y**
Is personal data collected, stored and used according to the principles of the GDPR?	**Y**

Principal Mrs M. McCahery Cert Ed **Headmaster** Joe Knight BA Hons, PCGE, NPQH
24 Thornton Road, London, SW12 0LF
020 8674 9514 office@whitehouseschool.com
www.whitehouseschool.com