



WALTHAMSTOW HALL  
SEVENOAKS

## **E-SAFETY POLICY FOR STAFF AND STUDENTS**

**This policy forms one of a suite of policies at Walthamstow Hall for safeguarding children.** It should be seen alongside and read in conjunction with the Walthamstow Hall Anti-Bullying (including cyber-bullying) Policy, the Bring Your Own Device Policy, Curriculum Policy, Safeguarding (Child Protection) Policy, Data Protection Policy and Behaviour and Sanctions Policy.

This policy has been drawn up with regard to the latest version of Keeping Children Safe in Education and has regard to the duties outlined in the Prevent Duty (DfE advice for schools, June 2015).

Both this policy and the Acceptable Use Policy (for all staff and pupils) cover both fixed and mobile internet devices provided by the School (such as PCs, laptops, webcams, tablets, whiteboards, digital video equipment, etc.); as well as all devices owned by pupils, staff, or visitors and brought onto school premises (personal laptops, tablets, smart phones, etc.).

This policy also provides safeguards and rules to guide all users – whether staff or students – in their online experiences (Appendices I - 10). E-Safety is primarily about protecting children whilst they are in the care of the School and educating them for when they are not. It underlines the need to educate children and young people about the benefits and risks of using new technologies both in and out of School.

An e-Safety Audit (Appendix I) has been carried by the Headmistress and Senior Management Group (November 2023) to ascertain whether the relevant requirements for e-safety are in place at Walthamstow Hall. The Headmistress has overall responsibility for this e-safety policy. She will work with the Director of Digital Services and Innovation and the Deputy Heads to whom day-to-day responsibility has been delegated along with the Safeguarding Governor whose responsibility includes e-safety, to oversee the implementation of this policy.

### **I. Online Safety**

It is essential that children are safeguarded from potentially harmful and inappropriate online material. The breadth of issues classified within online safety is considerable, but can be categorised into four areas of risk:

- **Content:** being exposed to illegal, inappropriate or harmful content, for example: pornography, targeted misinformation, racism, misogyny, self-harm, suicide, anti-Semitism, radicalisation and extremism.
- **Contact:** being subjected to harmful online interaction with other users; for example: peer to peer pressure, commercial advertising and adults posing as children or young adults with the intention to groom or exploit them for sexual, criminal, financial or other purposes.
- **Conduct:** personal online behaviour that increases the likelihood of, or causes,

harm; for example, making, sending and receiving explicit images (e.g consensual and non-consensual sharing of nudes and semi-nudes and/or pornography, sharing other explicit images and online bullying.

- **Commerce:** risks such as online gambling, inappropriate advertising, phishing and or financial scams. If we feel our pupils, students or staff are at risk, it will be reported it to the Anti-Phishing Working Group (<https://apwg.org/>).

Where referenced, “Unauthorised Purposes” refers to the accessing, distributing or creation of material that falls within any of the categories listed above.

## **2. The use of the Internet to enhance and extend teaching and learning:**

- Pupils are taught what Internet use is acceptable and what is not. They are given clear objectives for Internet use as appropriate. Safe use of the Internet is embedded in the PSHEE programme.
- Internet use is planned to enrich and extend learning activities.
- Pupils are educated in the effective use of the Internet for research, including the skills of knowledge location, retrieval and evaluation.
- Pupils are shown how to publish and present information to a wider audience.
- Pupils are taught how to be critically aware of the materials they are shown and how to evaluate Internet content to assess its accuracy and validity.

The School will do its utmost to ensure that the use of Internet derived materials by staff and pupils complies with copyright law.

## **3. Digital system security**

- The School’s DIGITAL systems’ security is reviewed regularly and modified as necessary.
- Virus protection is installed and updated regularly.
- The servers’ operating system is secured and is kept up to date.
- Access to the School’s wireless network is proactively managed and is secured.
- The BYOD Policy gives access to the School network via users’ own devices. This is allowed only through Account credentials and Group Membership.
- Files held on the School’s network are regularly checked.
- The Director of Digital Services and Innovation will review system capacity regularly and take appropriate action.
- The School monitors email traffic and blocks spam and certain attachments.
- The use of user logins and passwords is compulsory, with a minimum password length.
- When staff or students leave the School, their login accounts will be disabled on leaving if during the academic year or on 30<sup>th</sup> August if leaving at the end of the Academic year. Their personal work areas will be retained for one academic year before being removed. Backups of work areas, emails and other Digital footprint items will be retained for up to 7 years.

## **4. Authorised Internet access**

- The School maintains a current record of staff and pupils who are granted Internet access.

- All staff are required to sign the Staff Information Systems Code of Conduct (Appendix 4).
- Parents are informed that pupils will be provided with supervised Internet access (Junior School) and monitored access (Senior School). They are asked to sign and return a consent form for pupil access. (Appendices 2 and 3).
- Pupils must agree to and comply with the Acceptable User Policy statement each time they access a School computer.

## **5. Unsuitable sites**

- If staff discover any unsuitable websites, the URL, time, and content must be reported to the Director of Digital Services and Innovation.

## **6. E-Mail**

- Pupils must tell a member of staff immediately if they receive an offensive e-mail. They will then inform the Director of Digital Services and Innovation (or, in the Junior School, the Deputy Head who will in turn inform the Director of Digital Services and Innovation ) who will take the appropriate course of action.
- Pupils must not reveal personal details of themselves or others in e-mail communication or arrange to meet anyone without specific permission.
- Access in School to external e-mail accounts will be blocked with the exception of Sixth Form students.
- Incoming e-mail should be treated as suspicious and attachments not opened unless the author is known.
- The forwarding of chain letters is not permitted.
- Staff and pupils may access their School emails externally. All internal policy rules extend to this use too. On no account must user login details be revealed to unauthorised persons.
- Mass emailing of distribution lists is limited through approved sender lists.

## **7. Social Networking and Social Media**

- The School controls and restricts access to all social networking and social media sites while connected to, or making use of, school hardware and connections.
- Pupils are educated in the safe and courteous use of social networking sites when they are not in School (Appendix 9). In particular they will be advised:
  - Never to give out personal details of any kind which may identify them or their location.
  - Not to place personal photographs on any social network space.
  - To set passwords, deny access to unknown individuals and instructed how to block unwanted communications.
  - To invite known friends only and deny access to others and to make their profiles private.
  - To make use of Multi-Factor Authentication where available.
- Parents are advised that the use of social network spaces outside School brings a range of dangers for pupils of all ages, but particularly those of Junior School age. Information will be supplied to parents on a regular basis alerting them of anything relevant to home Internet use.

- While the School's Virtual Learning Environment (VLE) Platform is able to embed various social media feeds onto pages directly, staff are directed to utilise screenshots to share useful social media content to students rather than live links. While Social media content itself can be harmless, it is often the replies and comments on social media that risk exposure to content that breaches the guidelines given above regarding Content, Contact, Conduct and Commerce. The School provides space for departments on the VLE. Blogs and forums must be configured to prevent un-moderated content or comments appearing.
- Staff official blogs and social media feeds are discouraged and discussion should be had with the Director of Marketing before launching any initiative involving the use of Social Media. Where permission has been given, accounts must be password protected with multi-factor authentication. Usernames and Passwords for these accounts must be made available to the Director of Marketing. Members of staff must not run social network spaces for pupils on a personal basis.
- Newsgroups will be blocked.
- Staff personal use of social networking, social media and personal publishing sites will be discussed as part of staff induction and safe and professional behaviour is outlined in Staff Code of Conduct.

## **8. Filtering**

- The School continuously filters the content of Internet sites accessed within School in order to protect pupils from unsuitable materials. As far as possible, the level of filtering is appropriate to the age of the pupil. There are several levels of filtering: Junior School, Key Stage 3, Key Stage 4 and Key Stage 5.
- Regular checks will be made to ensure that the filtering methods are appropriate, effective and reasonable.
- School filters and the DIGITAL Acceptable Use policy have been checked to ensure that pupils are safe from terrorist and extremist material when accessing the internet in School.
- The Internet security system currently used by the School means that any Wi-Fi capable device brought into School by pupils in Key Stage 3 cannot access the School network or the Internet without specific permission from the Head of Learning Strategies and Director of Digital Services and Innovation.

## **9. Remote Learning**

- When delivering remote learning, staff will:
  - Only use online tools that have been evaluated and agreed by leadership.
  - Ensure remote learning activities are planned in accordance with our curriculum policies, taking learner needs and technology access into account.
- If remote learning is taking place 'live' using webcams or chat facilities, staff and learners will ensure a professional environment is maintained. This means:
  - Staff will record the length, time, date and attendance of any online lessons/contact held or made.
  - Sessions will not be delivered in any 1:1 situation, unless pre-approval has been given by the DSL and/or Deputy DSL and the session is auditable.

- Staff will record any online lessons so they can be audited or accessed later if required; learners and staff will be made aware that lessons are being recorded. Please also refer to the School policy on Taking, Using and Storing Images and Video of Children.
- Staff will agree online behaviour expectations with learners at the start of lessons.
- Staff will revisit the **Acceptable Use of Technology Policy** with learners as necessary.
- All participants will wear suitable dress, use professional language, and ensure backgrounds of videos (live or pre-recorded) are neutral and appropriate.
- Staff and learners should ensure personal information and/or, inappropriate or unsuitable personal items are not visible.
- Where possible, other household members should not be in the background or shot; if this unavoidable, they should follow appropriate language and behaviour expectations.
- If Live streaming, staff will mute and/or disable learners' videos and microphones, as required.

#### **10. Published content on the School website**

- The contact details on the School website include the School address, e-mail and telephone number. Staff or pupil personal information is not published.
- The Headmistress - in conjunction with the Director of Marketing and Alumnae - takes overall editorial responsibility and ensures that content is accurate and appropriate.

#### **11. Publishing students' images and work**

- Photographs that include pupils are selected carefully and are appropriate for the context.
- Pupils' full names are not normally to be used anywhere on the School website, particularly in association with photographs.
- Written permission from parents or carers is obtained before photographs of pupils are published on the School website.

#### **12. Protecting personal data**

- Personal data is recorded, processed, transferred and made available according to the Data Protection Act 2018 and UK GDPR. For further information please see the Records Retention and Storage Policy.

#### **13. Assessing risks**

Walthamstow Hall will take all reasonable precautions to prevent access to inappropriate material. However, due to the international scale and breadth of content, it is not possible to guarantee that unsuitable material will never appear on a School computer. The School cannot accept responsibility for the material accessed, or any consequences of Internet access.

The School aims to audit use regularly to establish if the e-safety policy is adequate and that the implementation of the e-safety policy is appropriate and effective.

It is the responsibility of the Director of Digital Services and Innovation, in conjunction with the rest of the staff, to remain aware of developments in technology, systems or protocols that will affect the accessibility of, or exposure to, content falling within the categories outlined in the “Online Safety” section.

#### **14. Handling e-safety complaints or concerns**

- Complaints of Internet misuse will be taken very seriously and will be dealt with by the relevant Head of Key Stage or Deputy Head.
- Any complaint about staff misuse must be referred to the Headmistress.
- An e-safety concern which relates to Child Protection including concerns relating to Prevent, must be reported in accordance with the School’s Safeguarding (Child Protection) Policy and procedures.
- Pupils and parents will be informed of the complaints’ procedure.

#### **15. Communication of policy**

##### **A. Pupils**

- E-safety rules are posted in all rooms where computers are used and discussed with pupils regularly.
- A Code of Conduct for use of School Computers and Guidelines for using Email and sending Text Messages are printed in each pupils’ Student Planner.
- Pupils are informed that network and Internet use is monitored and any misuse will be followed up with appropriate action.
- An appropriate programme of e-safety training will be provided for all pupils, some of which will be based on the ‘Think U Know’ materials from CEOP (Child Exploitation and On-line Protection Centre). This is embedded in the PSHEE curriculum.

##### **B. Staff**

- All staff are informed of Walthamstow Hall’s e-safety policy and its importance explained. For example, teaching staff are made aware of the risks posed by online activity of extremist and terrorist groups.
- All staff should be aware safeguarding issues can manifest themselves via peer-on-peer abuse. This is most likely to include, but not limited to, bullying (including cyber bullying)
- Staff should be aware that Internet traffic can be monitored and traced to the individual user. Discretion and professional conduct are essential.

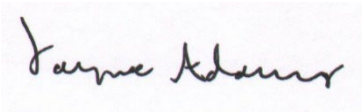
##### **C. Parents**

- Parents’ attention will be drawn to the School’s e-Safety Policy in newsletters, on the School website and in any other relevant literature.
- The School maintains a list of e-safety resources for parents on the School website (Appendix 6b). There is also a link on the School website to CEOP (Child Exploitation and Online Protection Centre) for reporting internet abuse.

- The School requires all new parents to sign the parent/pupil agreement when they register their child with the School. (Appendix 3)

This policy will be reviewed and updated regularly.

Revised: November 2023  
Next Review Date: November 2024

Signed by: .....  ..... Date: ...17 November 2023.....  
Mrs J Adams  
Chairman of the Governing Body



## **E-SAFETY POLICY FOR STAFF AND STUDENTS**

### **Appendices**

Appendix 1	e-Safety Audit
Appendix 2	e-Safety Rules
Appendix 3	e-safety Rules – Parent and Pupil Agreement
Appendix 4	Staff Information Systems Code of Conduct
Appendix 5	Walthamstow Hall Staff Laptop Loan Agreement
Appendix 6	Useful e-Safety resources: (a) staff (b) parents
Appendix 7	Procedure for reporting misuse
Appendix 8	Incident Record
Appendix 9	Senior School e-Guidelines (in the pupil planner) Code of Conduct for use of School Computers Guidelines for using email and sending text messages Guidelines for using a mobile phone and social networking Junior School e-Guidelines (in the pupil Planner) Code of Conduct for School Computers – KS2 Code of Conduct for School Computers – KS1 Code of Conduct for School Computers – Reception





## **Walthamstow Hall E-Safety Audit**

Has the School an e-Safety Policy that complies with latest guidance?	Yes
Date of latest review:	November 2023
The Policy was agreed by Governors on:	17 November 2023
The Policy is available for staff at:	\\Central Resource Library\\AA-Staff\\School Policies
And for parents at:	School Website
The Designated Safeguarding Lead is:	The Headmistress
Has e-safety training been provided for both students and staff?	Yes. Regular staff updates, on-going for pupils via PSHEE
Do all staff sign a DIGITAL Code of Conduct	Yes
Do parents sign and return an agreement that their child will comply with the School e-Safety Rules?	Yes
Have school e-Safety Rules been set for pupils?	Yes
Are these Rules displayed in all rooms with computers?	Yes
Is Internet access provided by an approved education Internet service provider and complies with DfE requirements for safe and secure access?	Yes
Is personal data collected, stored and used according to the principles of the Data Protection Act 2018 and UK GDPR?	Yes
Are staff with responsibility for managing filtering, network access and monitoring adequately supervised by a member of SMG?	Yes



## Walthamstow Hall e-Safety Rules

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

- Users must not access a computer or the School networks for a purpose not permitted by the School.
- Irresponsible use may result in the removal/loss of network or Internet access.
- 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 in School must be appropriate to education.
- Emails should be written in accordance with the guidelines detailed in the Student Planners.
- Anonymous messages and chain letters are not permitted.
- Users must not reveal personal information through email, personal publishing, blogs or messaging.
- The School DIGITAL systems may not be used for private purposes, unless the Headmistress has given specific permission.
- On no account are any videos or photographs depicting School property, staff members or pupils in School uniform be uploaded on to any video-sharing or social networking websites such as YouTube, Facebook, Twitter, Tic-Toc etc without approval.
- Use for personal financial gain, gambling, political activity, advertising or illegal purposes is not permitted.
- The School Internet filtering systems must not be bypassed; the use of Proxies is not permitted and their use to attempt to circumvent internet filters can result in suspension of Wi-Fi access privilege.

*The School will exercise its right to monitor the use of the School's computer systems, including access to websites, 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.*



## e-Safety Parent Agreement - MSP

All pupils use computer facilities including Internet access as an essential part of their learning. Both pupils and their parents/carers are asked to sign to show that the E-Safety rules which are set out in the Parent Handbook have been understood and agreed. Pupils will sign an agreement when they start at Walthamstow Hall. The School's E-Safety Policy for Staff and Students is published on the [School's website](#).

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

- Users must not access a computer or the School networks for a purpose not permitted by the School.
- Irresponsible use may result in the removal/loss of network or Internet access.
- 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 in School must be appropriate to education.
- Emails should be written in accordance with the guidelines detailed in the Student Planners.
- Anonymous messages and chain letters are not permitted.
- Users must not reveal personal information through email, personal publishing, blogs or messaging.
- The School ICT systems may not be used for private purposes, unless the Headmistress has given specific permission.
- On no account will any videos or photographs depicting School property, staff members or pupils in School uniform be uploaded on to any video-sharing or social networking websites such as *Facebook, Instagram, Snapchat, TikTok, Twitter, YouTube* etc.
- Use for personal financial gain, gambling, political activity, advertising or illegal purposes is not permitted.
- The School Internet filtering systems must not be bypassed.

The School will exercise its right to monitor the use of the School's computer systems, including access to websites, 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.

Please tick to confirm that you have read and understood the School E-Safety rules and understood that the School will take all reasonable precautions to ensure that pupils cannot access inappropriate materials through the Internet. \* ☐





## Walthamstow Hall Staff Information Systems Code of Conduct

To ensure that staff are fully aware of their professional responsibilities when using information systems, they are asked to sign this Code of Conduct. Staff should consult the School's e-Safety Policy for further information and clarification.

- The information systems are School property and I understand that it is a criminal offence to use a computer for a purpose not permitted by its owner.
- I will ensure that my information systems use will always be compatible with my professional role.
- I understand that School information systems may not be used for private purposes, without specific permission from the Headmistress.
- I understand that the School may monitor my information systems and Internet use to ensure policy compliance.
- I will respect system security and I will not disclose any password or security information to anyone other than an appropriate system manager.
- I will not install any software or hardware without permission.
- I will ensure that personal data is kept secure and is used appropriately whether in School or accessed remotely, and only taken off the School premises on an appropriately secure or encrypted device.
- I will respect copyright and intellectual property rights.
- I will report any incidents of concern regarding children's safety to the Director of Digital Services and Innovation, the Designated Safeguarding Lead (DSL) or Single Point Of Contact (SPOC) for Prevent/Channel (the Headmistress) as appropriate.
- I will ensure that any electronic communications with pupils are compatible with my professional role.
- I will promote e-safety with pupils in my care and will help them to develop a responsible attitude to system use and to the content they access or create.
- I will ensure that I take all possible precautions to safeguard access to pupil data when out of School (e.g. when using ISAMS).

*The School may exercise its right to monitor the use of the School's information systems, including Internet access, the interception of e-mail and the deletion of inappropriate materials where it believes unauthorised use of the School's information 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.*

**I have read, understood and agreed with the Information Systems Code of Conduct**

Signed: .....Printed:..... Date: .....



## Walthamstow Hall Staff Laptop Loan Agreement

Laptops are provided on a need assessed basis to select staff. While the Laptop is in your care the following guidelines should be noted:

- The Laptop issued to you is the property of Walthamstow Hall (the School), loaned to you for the duration of your employment.
- You are the designated user of the Laptop allocated to you, identified by its serial number and any labels and codes applied by the IT department (which must not be removed or obscured).
- It is the responsibility of the designated user to inform the School as soon as reasonably possible (via the IT department) if the Laptop is lost, stolen or not functioning correctly. If the Laptop is lost, stolen or damaged you may be held liable if it is deemed that this was the result of negligence on your part.
  - Negligence in this case is defined as acting in a way that does not prevent foreseeable outcomes and includes (but is not limited to) leaving the Laptop on the roof of your car and driving away, leaving the Laptop in plain view in your vehicle whilst shopping resulting in theft or using the Laptop inappropriately which results in damage to the device.
- The Laptop must remain in your possession, should only be used by you and should be securely stored when not in use.
- The designated user must take all reasonable precautions to protect the content on the Laptop: a passcode must be enabled at all times.
- The Laptop may be used for personal reasons and have personal content (music, video, books, pictures, apps) installed or uploaded onto it, provided such use and content size is not significant. This can be monitored by the IT department.
- Personal content on the Laptop must not breach the standard DIGITAL user agreement nor be of a nature that could be found to be objectionable if seen by others.

The Laptop may be used for personal or professional internet use (web browsing, email, social networking etc.) provided any sites visited or content uploaded/downloaded is not of a nature that any other user would deem inappropriate.

- The School may request the return of the Laptop at any time and without notice, for inspection purposes or otherwise.
- The School carries no responsibility for the preservation of personal content.
- It is strongly recommended that any School content or material created or stored on the Laptop be saved to your network user space, through pre-specified means and hence backed up by the School system.
- Every care must be taken in the use of the Laptop to ensure that it is not lost or damaged, both on and off school grounds.
- All Laptop use must comply with the School e-Safety Policy and Data Protection Policy.

- It is acceptable to use the Laptop camera to video or photograph pupils engaging in School activities for the purposes of coaching, assessment or otherwise provided:
  - The activity complies with the School's health and safety policies and procedures.
  - The activity complies with the School's child protection policy.
  - That the photos/videos are only backed up to the School network system.
  - That the photos/videos are only stored for a period beyond the time required for their use on the School's network.

**Laptop Model & Name:**

.....

**Serial Number:** .....

**Network Manager: (signature)** ..... **Date:** .....

**Issued to:** .....

***I have read and understand the School's published guidelines on staff Laptop use and agree to abide by them.***

**Received By: (signature)** ..... **Date:** .....



## **Appendix 6(a) Useful Resources for Teachers**

BBC Stay Safe

<https://www.bbc.com/ownit>

Chat Danger

[www.chatdanger.com/](http://www.chatdanger.com/)

Child Exploitation and Online Protection Centre

<https://www.ceop.police.uk/Safety-Centre/>

Childnet

[www.childnet-int.org/](http://www.childnet-int.org/)

Cyber Café

[https://www.thinkuknow.co.uk/8\\_10/](https://www.thinkuknow.co.uk/8_10/)

Think U Know

<https://www.thinkuknow.co.uk/>

Principles of e-safety

<http://www.education.gov.uk/schools/pupilsupport/pastoralcare/b00198456/principles-of-e-safety>

UK Council for Internet Safety

<https://www.gov.uk/government/organisations/uk-council-for-internet-safety>

## **Appendix 6(b) Useful Resources for Parents**

Think U Know

<https://www.thinkuknow.co.uk/>

BBC Stay Safe

<https://www.bbc.com/ownit>

Childnet

[www.childnet-int.org/](http://www.childnet-int.org/)

Family Online Safe Institute

[www.fosi.org](http://www.fosi.org)

Internet Watch Foundation

[www.iwf.org.uk](http://www.iwf.org.uk)

UK Council for Internet Safety

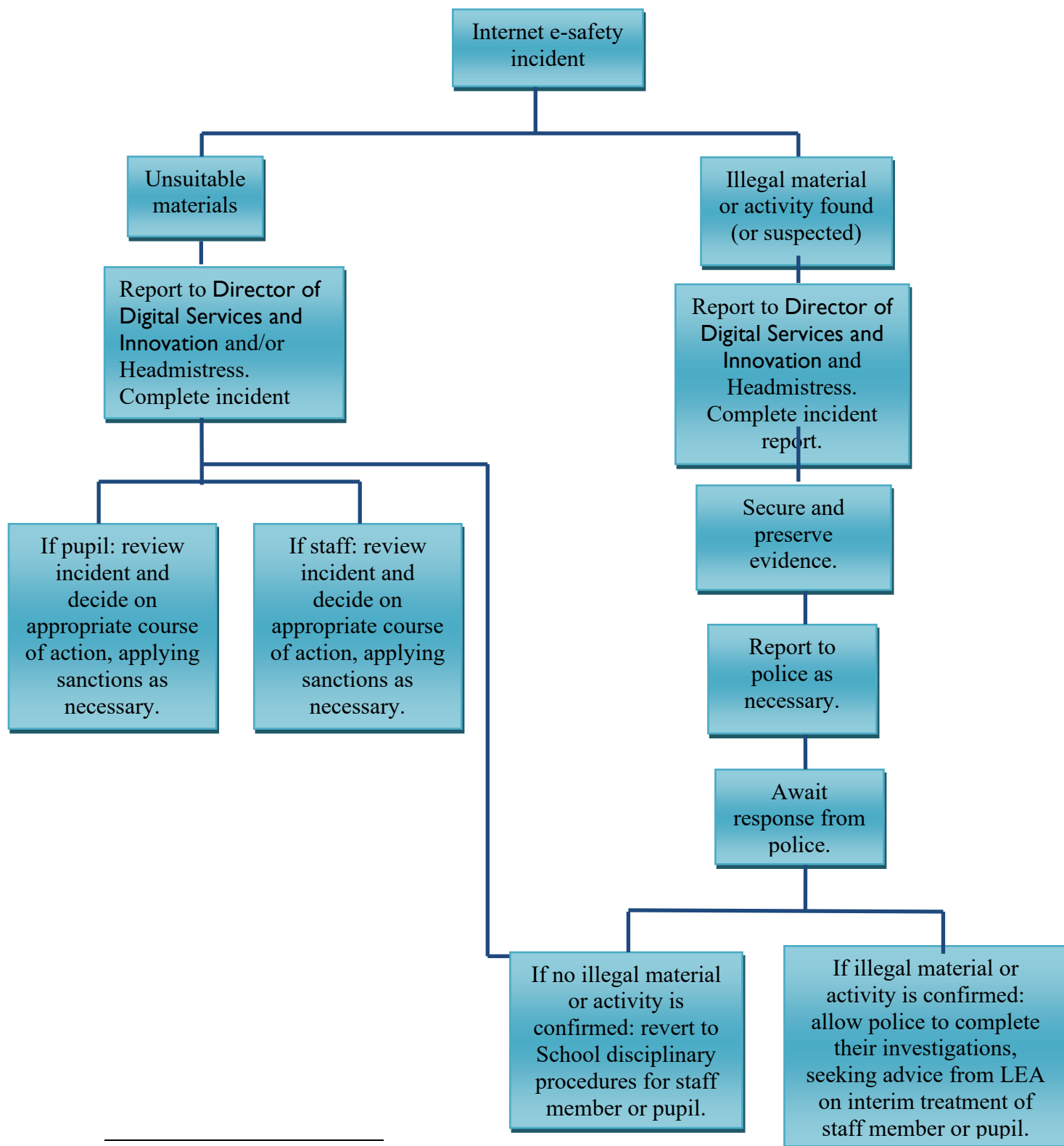
<https://www.gov.uk/government/organisations/uk-council-for-internet-safety>

Vodafone Digital Parenting Magazine

<https://www.vodafone.co.uk/mobile/digital-parenting>



## Flowchart for responding to Internet e-safety incidents<sup>1</sup> at Walthamstow Hall



<sup>1</sup> Consider whether Serious Incident Report to the Charity Commission, a report of a data breach to the Information Commissioner's Office or any other regulatory report is required



## Incident Record

<b>E-safety Incident</b>					<b>Date:</b>	<b>Time:</b>				
<b>Name of staff member discovering incident</b>										
<b>Pupil(s)/Staff member(s) involved</b>										
<b>Nature of Incident (Please tick relevant option)</b>	Accidental access to inappropriate material	<input type="checkbox"/>	Intentional access to inappropriate material	<input type="checkbox"/>	Cyber Bullying	<input type="checkbox"/>	Grooming	<input type="checkbox"/>	Other	<input type="checkbox"/>
<b>Details</b>										
<b>Time of event</b>	During a lesson		<input type="checkbox"/>	In unsupervised time		<input type="checkbox"/>	Outside school hours		<input type="checkbox"/>	
<b>Does the event warrant direct Police involvement (Yes if ...)</b>	Grooming	<input type="checkbox"/>	Violent Images	<input type="checkbox"/>	Pornographic Images	<input type="checkbox"/>	Other Criminal Activity	<input type="checkbox"/>		
<b>Headmistress/ Deputy Head</b>					<b>Date:</b>	<b>Time:</b>				
<b>STAFF Course of Action</b>	<b>Personnel Contact made with</b>		<b>Recommended Action</b>		<b>Action Applied</b>		<b>Chairman of Governors</b>			
<b>PUPIL Course of Action</b>	<b>Contacted Parents</b>	<input type="checkbox"/>	<b>Date:</b>	<b>Time:</b>						
	<b>Interviewed Parents/Carers</b>	<input type="checkbox"/>	<b>(Append Notes)</b>							
	<b>Recommended Action</b>				<b>Action Applied</b>					



## **Walthamstow Hall Code of Conduct for use of School Computers**

The School computers are available to help you with school work. You must keep to the following guidelines:

- Accept the 'Acceptable Use Policy' on the screen every time you log on and adhere to it.
- Only log onto the School network with your own user name and password and keep these confidential. If you think someone else knows this then you should ask for it to be changed.
- You are responsible for the content of your personal area and for ensuring that nothing unsuitable is stored. Computers are constantly monitored – including file contents, email activity, Cloud Storage, Remote Learning tools and Internet access.
- You must not attempt to gain access to anyone else's personal area.
- You must be very careful when using the Internet.
  - If you access an unsuitable site, exit immediately and do not forward material that could be considered inappropriate. Report any occurrences to the Director of Digital Services and Innovation.
  - Do not enter personal details on a website without permission.
  - The School operates a filter system and some sites are blocked for your safety.
  - You may **not** use chat rooms or social networking sites.
  - You must not attempt to bypass any of the School filtering.
  - You should check and preview work before printing so as not to waste resources.
  - You will be responsible for your behaviour when using the Internet. This includes resources you access and the language you use.
- You must ensure, to the best of your knowledge, that any data brought into School on memory sticks, CDs etc. is virus free.
- If you suspect a virus has entered the system, log off immediately and inform an IT Technician or your teacher.
- Do not download programs onto the School computers without permission.
- The computers are for school work, if you are not using them for their intended purpose you may be asked to log off to enable another pupil to use them for their school work.

- You will make sure that all DIGITAL communications with pupils, teachers or others is responsible and sensible.
- You will not give out any personal information such as name, phone number or address.
- You will not arrange to meet someone unless this is part of a School project approved by your teacher.
- Images of pupils and/or staff will only be taken, stored and used for School purposes in line with School policy and not be distributed outside the School network.
- On no account are any videos depicting School property, staff members or pupils in School uniform be uploaded on to any video-sharing or social networking websites such as YouTube, Facebook, Tic-Toc or Twitter.
- You will ensure that your online activity, both in School and outside School, will not cause the School, the staff, pupils or others distress or bring these into disrepute. Also bear in mind that any action you take online may stay in the public domain throughout your career/life and throughout the lives of anybody affected.
- Copyright and intellectual property rights must be respected.
- Failure to return a signed copy of this Code of Conduct will result in your IT access being removed until the School receives one.

It is important that we all follow these rules for your safety and in order to keep the school network running smoothly.

I agree to follow the code of conduct for the use of School computers.

**Signed:** \_\_\_\_\_ **Date:** \_\_\_\_\_



## **Walthamstow Hall**

### **Guidelines for using Email and sending Text Messages**

- An email or text message is a quick and generally informal i.e. relaxed, form of communication.
- Be aware that with an email or text, unlike a normal face to face conversation, you cannot see any facial expressions or hear any tone of voice.
- When sending or receiving emails and texts be aware of the following:
  - Messages, comments and/or images posted on-line are there permanently and cannot be deleted.
  - Think how the recipient will react when they receive the email or text – you will not be able to see the expression on their face. Likewise they cannot see yours as the sender.
  - In emails do not use all capital letters – it can appear as if you are ‘shouting’ and it is a lazy form of writing.
  - Humour or sarcasm are hard to convey in a written medium such as email or text, and a message which you meant to be funny can actually be hurtful or offensive. Think carefully about how what you write can be interpreted.
  - Do not send angry emails or texts; especially do not get involved in point-scoring via email or text.
  - If you have a disagreement with someone, or someone has upset you, never deal with it via email or text. Face to face conversation is the best way to resolve problems - it is much better to apologise whilst looking someone in the eye.
  - Be careful who you are sending emails to, generally only send to one recipient. Do not send bulk emails to students and staff and be careful when using the “Reply all” option.



## **Walthamstow Hall**

### **Guidelines for using a Mobile Phone & Social Networking**

#### **Mobiles**

- Think about whom you give your number to – you don't know where it might end up.
- If you receive a nasty text save it for evidence but don't reply to it, if you reply you are likely to get yourself into trouble too.
- Remember to be polite; try to talk quietly on mobiles in public places and keep your music quiet.
- A growing number of viruses are attacking mobile phones. Be careful what you download onto your mobile.
- If you often receive spam (junk mail) texts from random numbers report it to your mobile phone operator or Phone-paid Service Authority (<https://psauthority.org.uk/>)

#### **Social Networking**

Access to Social Networking Sites (SNS) is not allowed in School, but below are some guidelines for use out of School.

- Do **NOT** post images of staff or internal School views on any social networking site.
- Do **NOT** post any inappropriate images of yourself in School uniform or on School property on any social networking site.
- Always explore the privacy settings of your SNS to protect your privacy and to protect yourself from strangers.
- Get your friends and family to have a look at your SNS to check that you aren't giving out too much personal information or posting inappropriate photos/films because they might see something you've missed.
- Keep your passwords to yourself.
- Respect yourself and others online.
- If you are unlucky enough to have a bad experience online report it to the service provider and tell an adult.
- Cyberbullying is NEVER acceptable. If you or someone you know is targeted by bullies online tell them:
  - To report the bully to the website/service operator.
  - To keep evidence of the bullying behaviour.
  - To resist the temptation to reply to nasty messages.
  - To tell an adult.

Some web sites to visit that can provide extra information on Internet safety are:

<http://www.thinkuknow.co.uk>

<http://www.ceop.gov.uk>

<http://www.chatdanger.com>

<http://www.getsafeonline.org>



## **Walthamstow Hall Junior School**

### **Code of Conduct for use of School Computers – KS2**

The School uses computers to help you with your learning. The School wants you to stay safe when you are using the School network so you must follow the guidelines that are listed below:

- You must always ask permission from a teacher before you use any computer equipment in School.
- When you log onto the School network you must accept the code of conduct 'Acceptable Use Policy' on the screen every time you log on and do as it says.
- You must only log onto the School network with your own user name and password, if you are in Years 5 and 6 you must not tell anyone your password. If you think someone else knows your password then you should ask for it to be changed.
- You must not use another person's username and password.
- When you need to create a password make sure that it is not easy to guess.
- You must not deliberately look at other people's computer files without permission.
- You must always ask permission from a teacher before you use the Internet or use e-mail. You must ask permission before opening an e-mail or an e-mail attachment sent by someone you do not know.
- If you find something on the Internet that you do not like then you must tell your teacher.
- You must save your work in your own personal work area called your 'My Documents' or your S: drive.
- You must use School DIGITAL in a sensible and responsible way.
- You must do your best to look after School computer equipment properly.
- You must not use any computer CD/DVD or memory stick from home on any School computer without permission from a teacher.
- Mobile phones are not allowed in School unless, in exceptional circumstances, your parents have asked a member of the Junior Management Team for permission for you to bring it with you. If permission is given you must hand it in to the School office as soon as you arrive at School where it will be stored safely.

- You must not take digital photographs on School premises without permission from a teacher.
- You must not take or distribute images of anyone without their permission.
- You must not deliberately use DIGITAL to cause harm or be nasty to another person.
- Remember that the School keeps a record of everything that you do on the School network, the Internet sites you visit and all your e-mails.

I agree to follow the code of conduct for the use of School computers.

**Signed:** \_\_\_\_\_ **Date:** \_\_\_\_\_



## **Walthamstow Hall Junior School**

### **Code of Conduct for use of School Computers – KSI**

The School uses computers to help you with your learning. The School wants you to stay safe when you are using the School network so you must follow the guidelines that are listed below:

- You must always ask permission from a teacher before you use any computer equipment in School.
- When you log onto the School network you must accept the code of conduct on the screen every time you log on and do as it says.
- You must only log onto the School network with your own user name and password.
- You must not use another person's username and password.
- When you need to create a password make sure that it is not easy to guess
- You must not deliberately look at other people's computer files without permission.
- You must always ask permission from a teacher before you use the Internet or use e-mail. You must ask permission before opening an e-mail or an e-mail attachment sent by someone you do not know.
- If you find something on the Internet that you do not like then you must tell your teacher.
- You must save your work in your own personal work area called your 'My Documents' or your S: drive.
- You must use School DIGITAL in a sensible and responsible way.
- You must do your best to look after School computer equipment properly.
- You must not use any computer CD/DVD or memory stick from home on any School computer without permission from a teacher.
- Mobile phones are not allowed in School unless, in exceptional circumstances, your parents have asked a member of the Junior Management Team for permission for you to bring it with you. If permission is given you must hand it in to the School office as soon as you arrive at School where it will be stored safely.



- You must not take digital photographs on School premises without permission from a teacher.
- You must not take or distribute images of anyone without their permission.
- You must not deliberately use DIGITAL to cause harm or be nasty to another person.
- Remember that the School keeps a record of everything that you do on the School network, the Internet sites you visit and all your e-mails.

I agree to follow the code of conduct for the use of school computers.



## **Walthamstow Hall Junior School**

### **Code of Conduct for use of School Computers – Reception**

The School uses computers to help you with your learning. The School wants you to stay safe when you are using the School network so you must follow the guidelines that are listed below:

- You must always ask permission from a teacher before you use any computers in School.
- Your teacher will help you log onto a computer with your own user name and password.
- You can only use the Internet when a teacher is with you.
- You can click on the buttons or links on the computer when you know what they do.
- If you see something on the Internet that you do not like then you must tell your teacher.
- You must ask your teacher when you want to save a pDigitalure or some writing.
- You must look after the School computers in a sensible and responsible way.

**I will try and remember what I must do with the School computers.**