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 BYOD (Bring Your Own Devices) Policy, Curriculum Policy, Safeguarding (Child Protection) Policy, Data Protection, and Behaviour Policy.

This policy has been drawn up with regard to Keeping Children Safe in Education 2021, the document 'E-Safety: developing whole School policies to support effective practices' produced by BECTA 2005 along with 'Kent Schools Core e-Safety Policy and Audit 2008' and KCC Schools and Settings e-Safety Policy Template 2012 which is approved by the KCC Children, Families, Health and Education Directorate and produced by Kent County Council in conjunction with Kent Police. This policy also has regard to the duties outlined in the Prevent Duty (DfE advice for schools, June 2015).

This policy covers the safe use of the Internet and electronic communications technologies such as mobile phones and wireless connectivity. It highlights the need to educate children and young people about the benefits and risks of using new technologies both in and out of School. It also provides safeguards and rules to guide all users – whether staff or students – in their online experiences. (Appendices 1 - 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.

An e-Safety Audit (Appendix 1) has been carried by the Headmistress and Senior Management Group (in September 2021) 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 e-Safety Officer who is the Network Manager along with the Deputy Heads to whom day-to-day responsibility has been delegated and the Governor responsible for e-safety to oversee the implementation of this policy. The Assistant Head of the Junior School is responsible in the first instance for e-safety on the Junior School site.

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, fake news, 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; and
- **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/).

Why the Internet and digital communications are important:

- The Internet is an essential element in 21st century life for education, business and social interaction. The school has a duty to provide students with high-quality Internet access as part of their learning. It also has a duty to ensure that students are given the necessary information and expertise to ensure it is used responsibly, safely and securely, both in and out of school.
- The Internet is essential to support the professional work of teaching and to enhance the school's management information and administration systems.

The benefits of Internet use:

- Access to learning wherever and whenever convenient.
- Access to world-wide educational resources including museums and art galleries.
- Educational and cultural exchanges between students world-wide.
- Access to experts in many fields for students 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.
- Exchange of data and information with relevant bodies such as ISC (Independent Schools Council).

The use of the Internet to enhance and extend teaching and learning

- The School Internet access is designed expressly for student use and includes filtering appropriate to the age of students.
- Students 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.
- Students are educated in the effective use of the Internet for research, including the skills of knowledge location, retrieval and evaluation.
- Students are shown how to publish and present information to a wider audience.
- Students 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.

Managing Internet access

1. Information system security

- The School's ICT systems security are 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 with a minimum WPA2 encryption.
- The BYOD Policy gives access to the School network via users' own devices. This is allowed only through Active Directory Account credentials and Group Membership
- Files held on the School's network are regularly checked.
- The Network Manager will review system capacity regularly and take appropriate action.
- The Network Manager 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 and their personal work areas is retained for one academic year before being removed.

2. Authorised Internet access

- The School maintains a current record of staff and students who are granted Internet access.
- All staff are required to sign the Staff Information Systems Code of Conduct (Appendix 4). Staff who are provided with School laptops and / or iPads must sign the Walthamstow Hall Staff Laptop Loan Agreement (Appendix 5) and/or the Staff iPad Loan Agreement (Appendix 10).
- Parents are informed that students 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 student access. (Appendices 2 and 3).
- Students must agree to and comply with the 'Responsible Computer Use' Acceptable User Policy statement each time they log on to a School computer.

3. Unsuitable sites

If staff discover any unsuitable websites, the URL (Website address), time, and content must be reported to the Network Manager who is the School's e-safety officer.

4. E-Mail

- Students may only use approved e-mail accounts on the School system.
- Students must tell a member of staff immediately if they receive an offensive e-mail. He/she will then inform the Network Manager (or, in the Junior School, the Assistant Head of the Junior School who will in turn inform the Network Manager) who will take the appropriate course of action.
- Students 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 (Sixth Form will be allowed to access external e-mail accounts).

- Incoming e-mail should be treated as suspicious and attachments not opened unless the author is known.
- E-mails sent to parents should be written carefully and be authorised before sending, for example, by one of the Junior Management Team in the case of the Junior School, in the same way as a letter written on School headed paper.
- The forwarding of chain letters is not permitted.
- Staff and students 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.

5. Social Networking and Social Media

- The School controls and restricts access to all social networking and social media sites.
- Students 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.
- Parents are advised that the use of social network spaces outside School brings a range of dangers for students 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.
- Where possible Staff wishing to use social media tools with students as part of the curriculum should use the tools embedded into the School's VLE. However, if they wish to use sites such as Twitter then they will risk assess the sites before use and check the terms and conditions to ensure the site is age appropriate. Staff will obtain approval from senior staff if they wish to use social media tools not embedded into the VLE.
- The School provides blogspace for departments for projects on the VLE. Blogs must be configured to prevent un-moderated content or comments appearing.
- Staff official blogs should be password protected. Members of staff are advised not to run social network spaces for students on a personal basis.
- Newsgroups will be blocked unless a specific use is approved.
- 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.

6. Filtering

- The School continuously filters the content of Internet sites accessed within school in order to protect students from unsuitable materials. As far as possible, the level of filtering is appropriate to the age of the student. There are several levels of filtering: staff, sixth-form, students Years 7-11, Early Years - year 6.
- Regular checks will be made to ensure that the filtering methods are appropriate, effective and reasonable. (UK Safer Internet Centre: KCSIE Sept 2021)

- School filters and ICT 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 mobile phones with Internet access or any personal laptops brought into School by students below Year 12 cannot access the School network or the Internet.

7. Emerging technologies

- Emerging technologies are evaluated for educational benefit along with any other implications as they develop and before their use is allowed in school.
- Portable devices such as mobile phones and iPads are increasingly sophisticated and these developments are monitored by the Headmistress in conjunction with the e-Safety Officer to ensure that they do not present a new route to undesirable material or communication.
    - The use of mobile phones and other personal devices by students and staff in school will be decided by the school and covered in the school's Acceptable Use Policy and Mobile Phone/BYOD policies.
    - The sending of abusive or inappropriate messages or content via mobile phones or personal devices is forbidden by any member of the School community and any breaches will be dealt with as part of the School discipline/behaviour policy.
    - Mobile phones will not be used during lessons or formal school time unless as part of an approved and directed curriculum activity with the consent of a member of staff.
    - The use of digital cameras (including those embedded into a personal device) is forbidden outside formal lessons.
    - The use of messaging services on Cellular enabled Watches is forbidden.
    - Electronic devices of all kinds brought into school are the responsibility of the user. The School accepts no responsibility for the loss, theft or damage of such items. Nor will the School accept responsibility for any adverse health effects caused by any such device either potential or actual.
    - Staff are advised not to use personal devices such as mobile phones, cameras or iPads to take photos or videos of students and to only use work-provided equipment for this purpose. More specific arrangements apply in the Junior School – see Junior School Mobile Phone Policy. If an occasion arises when a member of staff has to use their personal device to record images of students then the image should be transferred to school equipment as soon as possible and deleted from the personal device.
    - If a member of staff breaches the School policy then disciplinary action may be taken.
- Firefly is the School's Virtual Learning Platform and is used as an additional resource in teaching and learning
    - Staff will regularly monitor the usage of all aspects of Firefly by students and staff in all areas, in particular message and communication tools and publishing facilities.
    - All users will be mindful of copyright issues and will only upload appropriate content onto Firefly.

- When staff or students leave the School, their accounts to Firefly will be disabled.
- Any concerns about the content of Firefly may be recorded and dealt with in the following ways:
  - The user will be asked to remove any material deemed to be inappropriate or offensive.
  - The content will be removed by the site administrator if the user does not comply.
  - Access to Firefly for the user may be disabled.
  - The user will need to discuss the issue with SMG/Staff before reinstatement.

8. 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.
  - Where possible, pre-record content.

- 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.
  - Live sessions will involve at least two members of staff where possible. 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 made aware that lessons are being recorded. Please also refer to the School policy on Taking, Using and Storing Images of Children.
  - Staff will agree online behaviour expectations with learners at the start of lessons.
  - Staff will revisit our 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.

9. Published content on the School website

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

10. Publishing students' images and work

- Photographs that include students are selected carefully and are appropriate for the context.
- Students' 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 regularly before photographs of students are published on the School website.

11. Protecting personal data

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

Assessing risks

Walthamstow Hall 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. The School cannot accept responsibility for the material accessed, or any consequences of Internet access. The School aims to audit ICT use regularly to establish if the e-safety policy is adequate and that the implementation of the e-safety policy is appropriate and effective**.**

Handling e-safety complaints or concerns

- Complaints of Internet misuse will be taken very seriously and will be dealt with by the Junior Management Team or, in the Senior School, The Head of Lower School/ Middle School/ Sixth Form or a Deputy Head.
- Any complaint about staff misuse must be referred to the Headmistress.
- An e-safety concern which relates to Child Protection must be reported in accordance with the School's Child Protection Policy and procedures.
- Students and parents will be informed of the complaints' procedure.

Communication of policy

1. Students

- 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 student's Student Planner.
- Students 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 students, 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.

2. 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) (KCSIE Sept 2021)
- Staff should be aware that Internet traffic can be monitored and traced to the individual user. Discretion and professional conduct is essential.

3. 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)

Role responsibilities for Internet safety

Internet safety is a whole School responsibility but key individuals have specific responsibilities outlined below:

The Headmistress

The Headmistress has ultimate responsibility for e-safety issues within the School. In addition, she will ensure that:

- The Governing Body is kept informed of any relevant e-safety issues.
- There is appropriate funding to support Internet safety activities throughout the School for both the technical infrastructure and INSET training.
- Internet safety is promoted across the curriculum.

As the Designated Safeguarding Lead at Walthamstow Hall - the Headmistress - has responsibilities specific to that role which include:

- Participating in regular professional training on the safety issues relating to use of the Internet and related technologies.
- Ensuring that systems and procedures for supporting and/or referring on pupils as a result of breaches of Internet security are in place and are followed in any such cases.
- Under the Government's 'Prevent' strategy aimed at 'preventing people being drawn into terrorism', and thereby reducing the threat of terrorism to the UK, ensuring that all staff give due consideration to, and have an awareness and understanding of, the risk of radicalisation.

In practice the Headmistress delegates day-to-day responsibility for e-safety to the Deputy Head whose responsibilities include:

- Monitoring and reviewing Internet safety policies, practices and procedures and ensuring that management protocols for any incidents in which Internet safety is breached are responded to in an appropriate and consistent manner.
- Responding to e-safety updates using mechanisms such as https://www.e-safetysupport.com/ and http://www.saferinternet.org.uk/
- Liaising with the e-Safety Officer to create an on-going staff development programme. This includes written information on Internet safety, presentations at staff meetings and INSET Days and hands-on training sessions on practical aspects of Internet safety.

- Chairing an e-Safety Council that meets regularly with pupil representatives to listen to pupil views on e-safety and respond appropriately.

The Deputy Head work in conjunction with senior pastoral staff and the e-Safety Officer on matters of e-safety.

The Governing Body

The Governing Body has responsibility for child protection and health and safety, and elements of these will include Internet safety. An individual Governor will have specific responsibility for safeguarding, monitoring the implementation and effectiveness of the systems and policies then giving feedback to the Governing Body. They will be kept informed of e-safety policy and ensure that appropriate funding is authorised for Internet safety solutions, training and other activities as recommended by the Headmistress.

The E-Safety Officer

At Walthamstow Hall the Network Manager is the e-safety officer. He has a significant role to play in establishing and maintaining a safe ICT learning environment for the School. He has a high level of technical knowledge and expertise and their particular responsibilities include:

- Maintaining the School network at both the Junior and Senior School along with the technological measures for ensuring Internet safety.
- Liaising with the Headmistress, Deputy Head, Junior Management Team and any other relevant staff to ensure that educational and technological aspects of Internet safety support and complement one another.
- Ensuring that appropriate and effective electronic security systems are in place, such as filtering, monitoring and firewall technology, and virus protection supported by regular and thorough monitoring of computer networks.
- Documenting the location of all Internet-accessible computers within the School so that, in the event of a serious breach of Internet safety, detailed, up-to-date documentation of the breach is available as evidence if required.
- Ensuring that computers used by staff are secure.
- Carrying out regular checks for indications of misuse and reporting any abuse according to correct procedure. (Appendix 7)
- Reporting any illegal or indecent material found on the school network immediately to the police, via the Headmistress. In such an event he will ensure that all relevant evidence is secured and preserved in order that any potential criminal proceedings are not compromised.
- Maintaining an appropriate level of professional conduct in their own Internet use both within and outside school.
- Reviewing the ICT Code of Conduct on a regular basis in conjunction with senior staff.

Heads of Department (Senior School) / Subject Leaders (Junior School)
Heads of Department and subject leaders have an important role to play in developing a safe ICT learning environment in schools and they play a key part in supporting the Internet safety culture within the School. In particular they are responsible for:

- Developing additional Internet safety policies where necessary within the department/subject area.
- Ensuring a co-ordinated approach across the subject/department to teaching Internet safety issues, making sure that they are in line with School policy.
- Working with relevant staff, e.g. the Librarians, to develop resource-based learning experiences to enable students to develop their information literacy skills within the context of the curriculum.
- Follow the correct procedure if there is any misuse of computers within their departmental/subject areas.
- Raising any matters relating to Internet safety at departmental meetings, at Junior School staff meetings or during classroom teachers' individual performance appraisals.

Pastoral leaders and form tutors
The pastoral team plays an important role and it is essential that all of them are involved in developing a safe ICT learning environment. In particular they are responsible for:

- Developing and maintaining knowledge of Internet safety issues, particularly with regard to how they might affect students.
- Ensuring any instances of ICT misuse, whether accidental or deliberate, are dealt with through the proper channels. (Appendix 8 Sample Incident Report)
- Acting as mediators for ICT-related incidents which occur outside School. This could involve working with students to ensure that any conflicts are resolved, ensuring that the perpetrators are aware of the seriousness of their actions, and that the victims receive the necessary support. It might also be necessary, on occasions, for the pastoral team to work with parents in reinforcing the Internet safety and acceptable use messages pupils receive within the home.

Classroom / subject staff
Classroom staff, particularly at Junior School level, spend a great deal of time with pupils and may have a considerable influence on their thinking and attitudes. They might be the first adults that a pupil approaches about any Internet safety matters. Additionally, classroom staff may notice a change in the behaviour and attitude of a pupil, which they suspect may be as a result of negative experiences on the Internet. In these cases, classroom staff should follow the appropriate referral process, seeking support as appropriate. In particular, classroom staff are responsible for:

- Developing and maintaining knowledge of Internet safety issues.
- Implementing school and departmental Internet safety policies through effective classroom practice.
- Ensuring any incidents of ICT abuse, whether accidental or deliberate, are dealt with through the proper channels.
- Ensuring that they provide the necessary support to pupils who experience problems when using the Internet.
- Planning classroom use of the Internet and ICT facilities to ensure that Internet safety is not compromised for example, evaluating websites in advance of classroom use and ensuring the school filtering levels provide appropriate protection for topics being studied.

- Embedding teaching of Internet safety messages within curriculum areas where possible.

School Librarians
The Libraries are an important resource and integral to the whole process of teaching and learning at Walthamstow Hall. They offer facilities for research, homework and personal study, including ICT. The Senior School Librarians contribute significantly to the Senior School curriculum through their work with students on information-handling skills, information literacy and independent research, for example. Where appropriate they will provide input to the e-safety officer on filtering and any other relevant issues.

Students/pupils
Students have their own personal responsibilities in creating a safe ICT learning environment. They should take responsibility for their own actions when using the Internet and other communications technologies. In particular they are responsible for:

- Upholding School policies relating to Internet safety and acceptable use of the Internet and other communications technologies.
- Developing their own set of safe and discriminating behaviours to guide them when they are online.
- Reporting any incidents of ICT misuse within School to the Network Manager or to a member of the teaching staff who should report it to the Network Manager.
- Seeking help or advice from a member of staff or the e-Safety Officer if they experience problems when online, or if they receive any content or contact which makes them feel uncomfortable in any way.
- Communicating with parents/carers about Internet safety issues and upholding any guidelines for safe and courteous Internet use in the home.

This policy will be reviewed and updated regularly.

Revised September 2021
Next Review Date September 2022

Signed by: …… Date: ……..
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 Student 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	e-Guidelines in the student planner (Senior School): Code of Conduct for use of School Computers; guidelines for using email and sending text messages; guidelines for using Instant Messaging accounts; guidelines for using a mobile phone and social networking. e-Guidelines in the Junior School Planner: Code of Conduct for School Computers – KS2; Code of Conduct for School Computers – KS1; Code of Conduct for School Computers – Reception
Appendix 10	Staff iPad Loan Agreement

Appendix 1

Walthamstow Hall E-Safety Audit

Has the School an e-Safety Policy that complies with latest guidance?	Yes
Date of latest review:	September 2021
The Policy was agreed by Governors on:	
The Policy is available for staff at:	\\Central Resource Library\AA-Staff\School Policies
And for parents at:	School Website
The designated Child Protection Officer is:	The Headmistress
Has e-safety training been provided for both students and staff?	Regular staff updates, on-going for students via PSHEE
Do all staff sign an ICT 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 students?	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?	Yes
Are staff with responsibility for managing filtering, network access and monitoring adequately supervised by a member of SMG?	Yes

***Appendix* 2**

Walthamstow Hall e-Safety Rules

These e-Safety Rules help to protect students 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 YouTube, Facebook, Twitter, Tic-Toc 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 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.

Appendix **3**

Walthamstow Hall
e-Safety Rules
Parent Agreement

All students use computer facilities including Internet access as an essential part of their learning. Parents are asked to sign to show that the e-Safety Rules have been understood and agreed.

Parent's Consent for Internet Access

I have read and understood the School e-Safety rules. I understand that the School will take all reasonable precautions to ensure that students cannot access inappropriate materials through the Internet.

Student:…… Form: ……...

Signed:……Date: ……

Please print name: ……

Please complete, sign and return to School

Appendix 4

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 School e-Safety Officer or the Designated Safeguarding Lead (DSL)/Single Point Of Contact (SPOC) for Prevent/Channel (the Headmistress).
- I will ensure that any electronic communications with students are compatible with my professional role.
- I will promote e-safety with students 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: ……

***Appendix* 5**

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 ICT 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

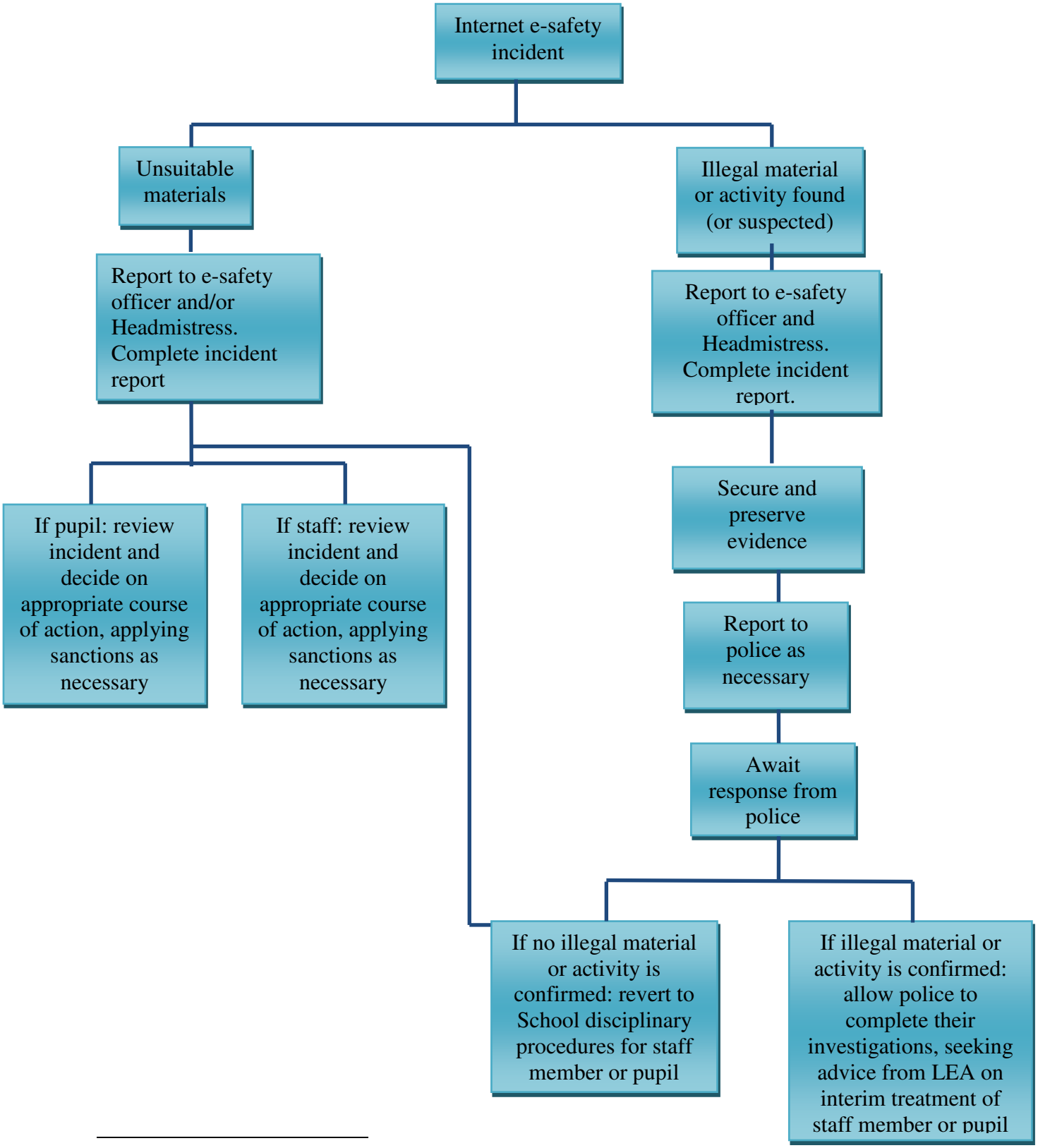
BBC Stay Safe
www.bbc.co.uk/cbbc/help/safesurfing/
Chat Danger
www.chatdanger.com/
Child Exploitation and Online Protection Centre
www.ceop.gov.uk/
Childnet
www.childnet-int.org/
Cyber Café
http://thinkuknow.co.uk/8_10/cybercafe/cafe/base.aspx
Digizen
www.digizen.org/
Kent e-Safety Policy and Guidance, Posters etc.
www.clusterweb.org.uk/kcn/e-safety_home.cfm
Kidsmart
www.kidsmart.org.uk/
Think U Know
www.thinkuknow.co.uk/
Principles of e-safety
http://www.education.gov.uk/schools/pupilsupport/pastoralcare/b00198456/principles-of-e-safety

Appendix 6(b) Useful Resources for Parents

Think U Know
www.thinkuknow.co.uk/
BBC Stay Safe
www.bbc.co.uk/cbbc/help/safesurfing/
Digizen
www.digizen.org/
Care for the family
www.careforthefamily.org.uk/pdf/supportnet/InternetSafety.pdf
Childnet
www.childnet-int.org/
Family Online Safe Institute
www.fosi.org
Internet Watch Foundation
www.iwf.org.uk
Kent leaflet for parents: Children, ICT & e-Safety
www.kented.org.uk/ngfl/ict/safety.htm
Internet Safety Zone
http://www.Internetsafetyzone.co.uk/parents/
Vodafone Digital Parenting Magazine
http://vodaphonedigital parenting.co.uk

Appendix 7

Flowchart for responding to Internet e-safety incidents[1] at Walthamstow Hall



[1] 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

Appendix **8**

Walthamstow Hall Sample Incident Record

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

Appendix 9

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 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 Network Manager
  - 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 in to 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 student to use them for their school work.

- You will make sure that all ICT 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 will 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 the 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 a 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 PhonepayPlus.

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.
    - 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 ICT 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 ICT 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 – KS1

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 ICT 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 ICT 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

EY2

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 you teacher when you want to save a picture 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.

Appendix 10

WALTHAMSTOW HALL
STAFF iPAD LOAN AGREEMENT

As part of the School's Development Plan it has been decided to provide a number of iPads for use by a designated member of each department to research the possible uses and benefits of an iPad for teaching and learning. While the iPad is in your care the following guidelines should be noted:

- The iPad and case 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 iPad 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 iPad is lost, stolen or not functioning correctly.
    - If the iPad 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 iPad on the roof of your car and driving away, leaving the iPad in plain view in your vehicle whilst shopping resulting in theft or using the iPad inappropriately which results in damage to the device
- The iPad may be 'remotely wiped' (all content deleted) by the IT department if the content is thought to be in jeopardy by the iPad being lost or stolen, or of a nature that an ordinary person would find objectionable.
- The iPad must remain in your possession, should only be used by you and should be securely stored when not in use
- The primary purpose of the iPad is to enhance teaching and learning and provide an alternative method of accessing the school MIS. It is an expectation that you will investigate how the iPad may benefit the teaching of your subject. This information must be shared with your department and SMT.
- Designated users must create an Apple ID for use on the iPad, with the designated user's School email address being used as the user name for that Apple ID.
- The School will provide a standard collection of applications (apps) for use on the iPad. IT will also provide some specific apps related to

your role or department. These apps must not be deleted from the iPad at any time

- New FREE DEMO apps that are educationally relevant may be installed. No paid apps may be installed. All requested paid apps will be reviewed and purchased by the IT department through the Apple VPP scheme.
- The designated user must take all reasonable precautions to protect the content on the iPad: a passcode must be enabled at all times
- The iPad 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 iPad must not breach the standard ICT user agreement nor be of a nature that could be found to be objectionable if seen by others
- The iPad 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 iPad at any time and without notice, for inspection purposes or otherwise
- The School carries no responsibility for the preservation of personal content; it is recommended that the iPad be backed up to iCloud
- It is strongly recommended that any school content or material created or stored on the iPad 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 iPad to ensure that it is not lost or damaged, both on and off School grounds
- The iPad must be enclosed in the provided case at all times.
- All iPad use must comply with the School e-Safety Policy and Data Protection Policy
- It is acceptable to use the iPad 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.
    - The photos/videos are not stored on the iPad for an extended period beyond the time required for their use (not more than 3 months).
    - 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.

iPad Model & Name:

……

Serial Number:

……

Network Manager: (signature) ……

Date: ……

Issued to: ……