



Woodford County
High School for Girls

SCHOOL POLICY

eSafety

Effective Date :	16/06/2016
Last modified :	16/06/2016
Document no	SP 03.07.003
Replaces Version :	25/06/2014
Approved: Full governors Meeting 16 th June 2016	Page 1 of 11

Table of Contents

Aims 1

Statutory Requirements..... 2

Policy Scope 2

Internet Access..... 2

Education and Training: 3

Security 5

Use of Digital and Video Images..... 5

Website: 6

Learning Platform: Fronter 7

CCTV: 7

Video Conferencing:..... 7

Managing Emerging Technologies 7

Prevent duty..... 8

Incidents and Response 8

Monitoring 9

Complaints 9

Review..... 9

Contacts 9

eSafety Incident Procedure..... 10

Aims

Woodford County High School recognises the benefits and opportunities which new technologies offer to teaching and learning.

We provide internet access to all our staff and students and encourage the use of technologies in all subjects in order to enhance skills and personal development. However the school acknowledges that the accessibility and global nature of the internet and different technologies available mean that there are potential risks and challenges associated with such use.

The school's approach is to implement appropriate safeguards within the school while supporting staff and students to identify and manage risk. We believe this can be achieved through a combination of security measures, training, guidance, ongoing support and through the implementation of our policies. In furtherance of our duty to safeguard students and to support the Every Child Matters agenda, Prevent Duty & Keeping Children Safe in Education we will take all reasonable steps to ensure that our staff and students stay e-safe and to satisfy our wider duty of care. This e-Safety policy should be read alongside other relevant school policies including Safeguarding, Anti Radicalisation, Acceptable Use, Anti Bullying and complaints policies.

Statutory Requirements

Data Protection Act 1998

Children Act 2004

Policy Scope

The policy applies to all Governors, staff and students of the school community (including temporary staff, volunteers, contracted support companies and community users) who have access to the schools IT systems, both on the premises and remotely. Any user of school IT systems must adhere to and sign a hard copy of the Acceptable Use Agreement.

The e-Safety Policy applies to all use of the internet this (includes mobile devices and wearable technologies) and forms of electronic communication such as email, mobile phones, camera phones, Ipads, tablets, social media sites etc. and will be provided to and discussed with all members of staff formally.

Internet Access

Woodford County High School is vigilant in its supervision of students use at all times, as far as is reasonable, and uses common sense strategies in learning resource areas where older students have more flexible access.

The school:

- Ensures that Internet access is filtered for all users
- Ensures that Internet filtering is set to keep children from seeing terrorist and extremist material.
- Ensures all staff and students understand that they must report any concerns to the safeguarding officer or Head Teacher
- Monitors usage to ensure students on school machines only publish within the appropriately secure school's Managed Learning Environment (MLE: Fronter)

- Requires teachers to be vigilant when conducting 'raw' image search with students e.g. Google image search and students are encouraged to report any issues
- Informs all users that internet use is monitored and logged
- Informs staff and students that that they must report any failure of the filtering systems directly to the Network Manager and or ICT Technician
- Requires students individually to sign an Acceptable Use Agreement Form which is fully explained and introduced as part of the teaching program
- Requires all staff to have read, understood and signed an Acceptable Use Agreement Form and keep a copy on file
- Requires all digital communications with students, pupils, parents should be on a professional level and only carried out using official school systems
- Ensures parents provide consent for students to use the Internet, as well as other ICT technologies, as part of the Acceptable Use Agreement Form signed at time of their daughters entry to the school
- Makes sure all users know and understand what the 'rules of appropriate use' are and what sanctions result from misuse – through staff meetings and the teaching program
- Keeps a record of any bullying or inappropriate behaviour for as long as is reasonable in-line with the school behaviour management system
- Ensures the named Child Protection Officer has appropriate training
- Provides advice and information on reporting offensive materials, abuse, bullying etc. to students, staff and parents
- Provides e-Safety advice and training for Governors, staff, students and parents
- Immediately refers any material we suspect is illegal to the appropriate authorities (Police and the Local Authority)

Education and Training:

Woodford County High School fosters a 'No Blame' environment that encourages students to tell a teacher or responsible adult immediately if they encounter any material that makes them feel uncomfortable.

The school:

- Teaches students and informs staff what to do if they find inappropriate web material i.e. to switch off monitor and report the URL to the teacher or Network Manager
- Ensures students and staff know what to do if there is a cyber-bullying incident
- Ensures all students know how to report any abuse (a report abuse button is also available in the e-Safety room on our MLE (Fronter and on the schools website)


Woodford County High School teaches e-Safety as part of the school curriculum, built on Local Authority and national guidance, expert external speakers are also invited into school to speak to

Governors, staff, students and parents. Students are taught a range of skills and behaviours appropriate to their age and experience, such as:

- to STOP and THINK before they CLICK
- to discriminate between fact, fiction and opinion
- to develop a range of strategies to validate and verify information before accepting its accuracy
- to skim and scan information
- to know how to narrow down or refine a search
- to understand how search engines work and to understand that this affects the results they see at the top of the listings
- to understand 'Netiquette' behaviour when using an online environment such as e-mail, to be polite, not to use bad or abusive language or other inappropriate behaviour to keep personal information private
- to understand how photographs can be manipulated and how web content can attract the wrong sort of attention should be careful in online environments
- to understand why on-line 'friends' may not be who they say they are and to understand why
- to understand why they should not post or share detailed accounts of their personal lives, contact information, daily routines, location, photographs and videos and to know how to ensure they have turned-on privacy settings
- to understand why they must not post pictures or videos of others without their permission
- to know that they should not download any files, such as music files, without express permission
- to have strategies for dealing with receipt of inappropriate materials
- to understand why and how some people will 'groom' young people for sexual reasons

The school emphasises that:

- when copying materials from the web, staff and students understand issues around plagiarism; how to check copyright and also know that they must observe and respect copyright and intellectual property rights
- staff and students understand the issues around aspects of the commercial use of the Internet, as age appropriate. This may include risks such as pop-ups, buying on-line, on-line gaming or gambling
- staff know how to send or receive sensitive and personal data and understand the requirement to encrypt data where the sensitivity requires data protection
- e-Safety training is provided to Governors, staff, students on a regular basis
- it provides advice, guidance and training for parents, by providing Information in school newsletters and weekly bulletins, via our parent room in Fronter (MLE), school web site and via groupcall messenger
- students will be taught about the impact of cyberbullying, sexting and trolling and know how to seek help if they are affected by any form of online bullying
- students will be made aware of where to seek help if they experience problems when using the internet and related technologies, i.e. parent or carer, teacher or trusted staff member, or an organisation such as Childline or the CLICK CEOP button

 <p>Woodford County High School for Girls</p> <p>SCHOOL POLICY</p> <p>eSafety</p>	Effective Date : 16/06/2016
	Last modified : 16/06/2016
	Document no SP 03.07.003
	Replaces Version : 25/06/2014
	Approved: Full governors Meeting 16 th June 2016

Security

Woodford County High School will do all that it can to make sure the school network is safe and secure. The Network Manager, will keep security software up to date. Appropriate security measures will include the use of enhanced filtering and protection of firewalls, servers, routers, work stations etc. to prevent accidental or malicious access of school systems and information. Digital communications, including email and internet postings, over the school network, will be monitored in line with the e-security policy

The school uses 'Smoothwall' an Internet Security and Content Filtering system which blocks sites that fall into categories such as pornography, race hatred, gaming, sites of an illegal nature, etc. All changes to the filtering policy are logged and only available to staff with the approved 'web filtering management' rights. All websites visited are logged and any breaches recorded, a daily report is automatically sent to the Head Teacher and Child Protection officer.

The school:

- uses individual, log-ins for all users and they are asked to keep this information secure
- uses Local Authority approved systems to send personal data over the Internet and uses encrypted devices or secure remote access where staff need to access personal level data off-site
- blocks all chat rooms and social networking sites except those that are part of an educational network or MLE:Fronter
- provides staff with a school email account for their professional use, and makes clear personal email should be through a separate account
- Provides students with a school email account for use in school, to enable them to communicate with staff and fellow students
- Students must inform a member of staff immediately if they receive items of an offensive nature electronically. Staff must inform a member of leadership if either a student reports such an event, or, they receive items of an offensive nature themselves.
- uses 'Netsupport: School' - a teacher remote-management control tool for controlling workstations, viewing users, setting-up applications and unrestricting or restricting internet web sites as required
- uses 'Netsupport: Technicians' – a console to remote-manage and assist staff and students for controlling workstations, viewing users, installing applications and unrestricting or restricting Internet web sites, where required

Use of Digital and Video Images

Woodford County High School gains parental permission for use of digital photographs, or video involving their daughter as part of the Parent-School Agreement when their daughter joins the school.


- We use video recording equipment on occasions in lessons as a tool to share best teaching practice. These recordings are used in school for teaching and will not use for any external purpose

Effective Date :	16/06/2016
Last modified :	16/06/2016
Document no	SP 03.07.003
Replaces Version :	25/06/2014
Approved: Full governors Meeting 16 th June 2016	Page 6 of 11

- Digital images or videos of students are stored in a teachers only shared images folder on the network and images are reviewed annually in the summer in order that those with no further use or relevance may be deleted
- We do not identify students in online photographic materials
- Staff sign the school's Acceptable Use Policy and this includes a clause on the use of mobile phones and personal equipment for taking pictures of students
- The school blocks or filters access to social networking sites unless there is a specific approved educational purpose
- Students are taught how images can be manipulated during lessons. Students are advised to be very careful about placing personal photos on any 'social' online network space. They are taught to understand the need to maintain privacy settings so as not to make public any personal information.
- Students are taught that they should not post or publish images or videos of others without their permission. We teach them about the risks associated with providing information with images (including the name of the file), that reveals the identity of others and their location, such as house number, street name or school. We teach them about the need to keep their data secure and what to do if they are subject to bullying or abuse.
- Parents may take photographs at school events. However, in doing so they must ensure that any images or videos taken involving children other than their own are for personal use only and will not be published in the public domain e.g. on the internet, social networking sites, etc.
- Staff and students are made aware that 'live streaming' using mobile device apps is not permitted in school.

Website:

- The Head teacher takes overall editorial responsibility to ensure that the website content is accurate and the quality of presentation is maintained
- Uploading of information is restricted to our website authorisers: e.g. Senior Leadership Team, Senior Administrative Office, School Business Manager and Network Manager
- The school web site complies with the school's guidelines for publications
- Most material is the school's own work; where other's work is published or linked to, we credit the sources used and state clearly the author's identity or status
- The point of contact on the web site is the school address, telephone number and we use a general email contact address, e.g. enquiries@woodford.redbridge.sch.uk. Home information or individual e-mail identities will not be published
- Photographs published on the web do not have full names attached
- We do not use student names when saving images in the file names or in the tags when publishing to the school website
- We expect teachers using school approved blogs or wikis to password protect them and run them from the school website

 <p>Woodford County High School for Girls</p> <p>SCHOOL POLICY</p> <p>eSafety</p>	Effective Date : 16/06/2016
	Last modified : 16/06/2016
	Document no SP 03.07.003
	Replaces Version : 25/06/2014
	Approved: Full governors Meeting 16 th June 2016

Learning Platform: Fronter

- Uploading of information on the school's MLE: Fronter is shared between different staff members according to their responsibilities
- Photographs and videos uploaded to the school's MLE: Fronter will only be accessible by members of the school community
- In school, students are only able to upload and publish within school approved and closed systems, such as the MLE: Fronter
- Teachers are instructed not to run social network spaces for student use on a personal basis or to open up their own spaces to their students, but to use the schools MLE: Fronter for such communications

CCTV:

- Woodford County High School has recording CCTV in the school sports block as part of our site surveillance for staff, student and hirer safety. We will not reveal any recordings without permission except where disclosed to the Police as part of a criminal investigation.

Video Conferencing:

Video Conferencing equipment may be used on occasion to link with other schools or external organisations; this encourages engagement and more active participation in the learning environment. Stimulating genuine dialogue between students and increases collaboration as well as providing an exciting, more dynamic learning experience.

- We will ensure pupils do not use video conferencing equipment unsupervised by a teacher or trained adult.
- Equipment is not kept in the classroom however, if this is bought into a classroom by a member of staff in advance of a Video Conference session this will be switched off when not in use and not set to auto answer.
- When recording a videoconference lesson, written permission should be given by all sites and participants. The reason for the recording must be given and the recording of videoconference should be clear to all parties at the start of the conference. Recorded material shall be stored securely.

Managing Emerging Technologies

- Emerging technologies are examined for educational benefit and risk assessments are carried out before use in school is allowed.

- Governors and the senior leadership team should note that technologies such as mobile phones with wireless internet access can bypass school filtering systems and present a new route to undesirable material and communications.

Prevent duty

- Woodford County High School is fully committed to safeguarding and promoting the welfare of all its pupils. Every member of staff recognises that safeguarding against radicalisation and extremism is no different to safeguarding against any other vulnerability in today's society.
- We protect children from the risk of radicalisation, by using filters on the internet to make sure they can't access extremist and terrorist material, or by vetting visitors who come into school to work with pupils.
- Our Safeguarding, Radicalisation and e-Safety policies set out our beliefs, strategies and procedures to protect vulnerable individuals from being radicalised or exposed to extremist views, by identifying who they are and promptly providing them with support.

Incidents and Response

Where an e-safety incident is reported to the school the matter will be dealt with very seriously. The school will act immediately to prevent, as far as reasonably possible, any harm or further harm occurring.

If a student wishes to report an incident, they can do so to their Form Tutor or to the school's e-safety Officer


Where a member of staff wishes to report an incident, they must contact their line manager as soon as possible. Following any incident, the school will review what has happened and decide on the most appropriate and proportionate course of action. Sanctions may be put in place, external agencies may be involved or the matter may be resolved internally depending on the seriousness of the incident (see pages 9 & 10).

CONTACT DETAILS:

Woodford County High School: 020 8504 0611

Safer Internet Centre: 0844 381 4772

Police (non-emergency): 0300 123 1212

 <p>Woodford County High School for Girls</p> <p>SCHOOL POLICY</p> <p>eSafety</p>	Effective Date : 16/06/2016
	Last modified : 16/06/2016
	Document no SP 03.07.003
	Replaces Version : 25/06/2014
	Approved: Full governors Meeting 16 th June 2016

Internet Watch Foundation (IWF): www.iwf.org.uk/

Child Exploitation & On-line Protection Centre (CEOP): <http://www.ceop.police.uk/safety-centre/>

Monitoring

Woodford County High School's Senior Leadership Team and the School's Governing Body will ensure that any relevant or new legislation that may impact upon the provision for e-safety within school will be reflected within this policy.

The Senior Leadership Team will be responsible for ensuring all members of school staff and students are aware of the existence and contents of the school e-safety policy.

Our school's e-safety procedures are reviewed by different stakeholders, including Governors, Senior Leadership Team, Child Protection Officer, Network Manager and ICT Steering Group Members (a cross-curricular group of teaching and non-teaching colleagues).

Complaints

Complaints will be dealt with in accordance with the school's complaints policy. Complaints relating to information handling may be referred to the Information Commissioner (the statutory regulator).

Further advice and information is available from the Information Commissioner's Office:

http://www.ico.gov.uk/for_organisations/data_protection/the_guide.aspx

Review

The policy will also be reconsidered where particular concerns are raised, where an e-safety incident has been recorded or to incorporate issues raised by emerging technologies.

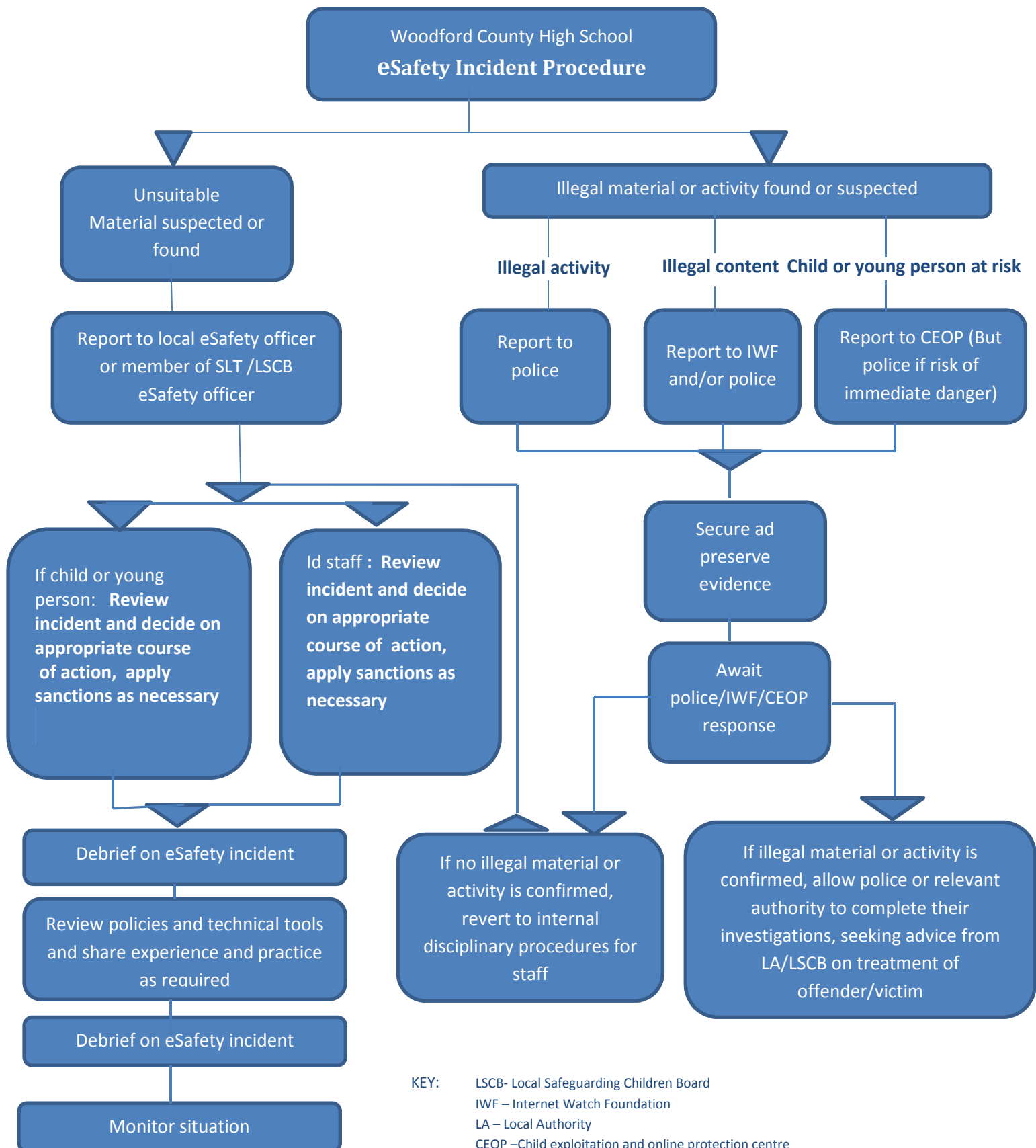
This policy will be monitored regularly with a full review being carried out annually by the Governing Body.

Contacts

If you have any enquires in relation to this policy, please contact the School Business Manager who will also act as the contact point for any subject access requests.



Effective Date :	16/06/2016
Last modified :	16/06/2016
Document no	SP 03.07.003
Replaces Version :	25/06/2014
Approved: Full governors Meeting 16 th June 2016	Page 10 of 11



KEY: LSCB- Local Safeguarding Children Board
IWF – Internet Watch Foundation
LA – Local Authority
CEOP –Child exploitation and online protection centre

Responding to eSafety Incidents
Flowchart of action

