Enfield County School

E-safety Policy

May 2017

Date Policy Updated:	May 2017
To Present to Governors:	May 2017
Date Policy Ratified:	June 2017
Date for next Review:	June 2018

1	**Introduction**	**3**
2	**Roles and Responsibilities**	**5**
3	**E-safety Development for Staff**	**7**
4	**School Infrastructure**	**8**
	Network Policy	8
5	**E-safety in the Curriculum**	**9**
6	**Password Security**	**10**
7	**Data Security**	**11**
	Sensitive Information and Confidentiality	12
8	**Managing Internet Access**	**13**
9	**Virtual Learning Environment (VLE)**	**14**
10	**Social Media Safeguards**	**15**
11	**Managing Emerging Technologies (Web 2.0)**	**16**
12	**Managing E-mail Communication**	**17**
13	**Mobile Technologies**	**18**
14	**Safe Use of Images**	**19**
15	**Misuse and Infringements**	**20**
16	**Acceptable Use Policy: Staff Agreement Form**	**21**
17	**Equal Opportunities**	**23**
18	**Parental Involvement**	**24**

1 Introduction

Enfield County is aware that the Internet and related technologies are powerful tools, which open up new prospects for communication and collaboration. Education is embracing these new technologies as they bring with them fresh opportunities for both teachers and learners.

Information and Communication Technology (ICT) is seen as an essential tool to support teaching and learning, as well as playing an important role in the everyday lives of children, young people and adults. At Enfield County we have incorporated these technologies in order to equip our students with the skills they will need for life-long learning and employment.

The world of ICT is a fast moving environment and covers a wide range of resources including; mobile learning, web-based learning and a Virtual Learning Environment (VLE) to name a few. Some of the technologies available to young people in/outside of school are:

- Computers, laptops and tablets
- Mobile phones
- Blogs & Wikis based on Web 2.0 technologies
- Online Forums
- Chat Rooms and Social Networking e.g. Instagram, Snapchat
- Music and Video Broadcasting
- Podcasting
- E-mail & Instant Messaging
- Virtual Learning Environment – Firefly
- Microblogging sites e.g. Twitter

While all these technologies are exciting and beneficial to the learner some of the web-based resources are hard to monitor and are not consistently policed. All users including adults need to be aware of the risks associated with the use of Internet technologies.

At Enfield County we take the matter of E-safety very seriously and we teach all our stakeholders in line with Enfield's Local Authority Safeguarding Children E-safety Policy how to use web-based technologies safely and legally. We teach our students the appropriate behaviours and thinking skills required for safe Internet use that will keep them safe in and beyond the classroom.

Our school website has a separate home page for E-safety and a range of materials are available for viewing/downloading for parents/carers and students. These documents link directly to CEOPS and Childnet advice leaflets so users can receive the most up to date material in relation to any E-safety issues.

This Acceptable Use Policy (AUP) and other related E-safety AUPs cover both fixed and mobile technologies within school (such as PCs, Laptops, PDAs, Tablets, Webcams, Smartphones, Voting Systems etc.) Please see AUP on page 21 of this document.

2 Roles and Responsibilities

E-safety is a very important aspect of strategic leadership at Enfield County and it is the responsibility of the Headteacher and Governors to ensure that the policy and practice of E-safety is embedded and monitored in our school. The named Designated Safeguarding Lead (DSL) at Enfield County is Ms J Scott and the DSL Deputy is Ms K Robbins. If they are unavailable please see Designated Officers, Mrs C Egleton, Mrs L Hayden or Ms P Rutherford (Headteacher). The DSL and DSL Deputy will deal with any E-safety or child protection issues that arise within the school.

Designated Officers (DSOs) ensure they keep up to date with E-safety issues and guidance through liaison with the Local Authority E-safety Officer and through organisations such as Child Exploitation and Online Protection (CEOP). The school's DSOs ensure the Headteacher, Senior Leadership and Governors are updated as necessary.

The school's ICT Steering Group has oversight of the E-safety policy and oversees the establishment and maintenance of a safe and secure e-learning environment at Enfield County School. Regular meetings are held to deal with any issues that arise concerning E-safety.

Governors need to have an overview and understanding of E-safety issues and strategies at the school. We ensure our governors are aware of our local and national guidance on E-safety and are updated annually on policy developments.

All teachers are responsible for promoting and supporting safe behaviours in their classrooms and following school E-safety procedures.

Students are required to be fully aware of the E-safety policy and this is covered in lessons.

Year Co-ordinators should keep matters of E-safety at the fore of any discussion with students regarding friendship problems. Central to this is fostering a 'No Blame' culture so students feel able to report any bullying, abuse or inappropriate materials.

All staff should be familiar with the school's policy including:

- Safe use of e-mail.
- Safe use of Internet including use of internet-based communication services, such as instant messaging and social networks.
- Safe use of school network, equipment and data.
- Safe use of digital images and digital technologies, such as mobile phones and digital cameras.
- Publication of student information/photographs and use of website.
- E-bullying / cyber bullying procedures.
- Their role in providing E-safety education for students.

Staff are reminded / updated about E-safety matters at least once a year and are required to sign the policy to accept the regulations.

This policy, supported by the school's AUPs for staff, visitors, governors and students, is to protect the interests of the whole school community.

Staff should understand that phone or online communications with students can occasionally lead to misunderstandings or even malicious accusations and must take care always to maintain a professional relationship.

3 E-safety Development for Staff

- New staff receive information on arrival of all the school's acceptable use policies and must sign and complete the relevant form before access is granted.
- All staff are made aware of the procedures that they must adhere to in the safeguarding of children within the context of E-safety and how to deal with any E-safety or misuse of ICT related technologies incidents.
- All staff are fully encouraged to embed E-safety activities within their curriculum area.
- Our staff receive regular information and training on E-safety issues via twilight sessions and the E-safety.
- Staff leaving the school will have their associated accounts removed.

4 School Infrastructure

Enfield County School has up-to-date anti-virus, anti-spyware and anti-spamware software and approved firewall solutions installed on our network. To make sure rogue applications are not downloaded and hackers cannot gain access to the school's equipment or into users' files through Internet use, students should not be able to download executable files and software.

All access to websites is controlled by a filter, WebScreen 2.0. Lists of blocked sites are maintained by our internet provider, London Grid for Learning (LGfL), and the suppliers of the product.

Unfortunately, inappropriate materials will inevitably get through any filtering system. We are vigilant and alert so that sites can be blocked as soon as they become apparent. Conversely, sometimes appropriate websites need to be unblocked. The network manager is able to block or liaise directly with LGfL over this.

High level monitoring of website access is also undertaken by Virgin and logs can be obtained where a site is under investigation.

We do not send personal data across the Internet unless it is encrypted or sent via secure systems such as the USO-FX or our approved learning platform, Firefly.

Network Policy

Enfield County School:

- Ensures network health through appropriate anti-virus software etc and network set-up so staff and students cannot download executable files such as .exe / .com / .vbs etc.
- Ensures their network is 'healthy' by having health checks regularly on the network.
- Ensures the network manager is up-to-date with services and polices.
- Ensures the network manager checks to ensure that the filtering methods are effective in practice and that they remove access to any website considered inappropriate by staff immediately.
- Never allows students access to Internet logs.
- Uses individual log-ins for students and all other users.
- Never sends personal data over the Internet unless it is encrypted or otherwise secured.
- Uses 'safer' search engines with students. 'Safe search' is enforced by the filtering system where appropriate.
- Ensures students only publish within appropriately secure learning environments such as their own closed, secure LGfL portal or learning platform.

5 E-safety in the Curriculum

- The school has a framework for teaching Internet skills in ICT and as a discrete subject in other areas.
- The school provides opportunities within a range of curriculum areas to teach about E-safety.
- Educating students on the dangers of technologies that may be encountered outside school is carried out informally when opportunities arise and is part of the E-safety curriculum.
- Students are aware of the relevant legislation when using the internet such as data protection and intellectual property, which may limit what they want to do but also serves to protect them.
- Students are taught about copyright and respecting other people's information and images etc. through discussion, modelling and activities.
- Students are aware of the impact of online bullying and know how to seek help if they are affected by these issues. Students are also aware of where to seek advice and help if they experience problems when using the internet and related technologies; i.e. parent/carer, teacher/trusted staff member, ECS website E-safety homepage, or an organisation such as Childline/CEOP report abuse button.
- Students are taught to critically evaluate materials and learn effective searching skills through cross curricular activities discussions and via the ICT curriculum.
- E-safety rules will be posted in all rooms where computers are used.
- All system users will be informed that network and Internet use will be monitored.

6 Password Security

- When accessing any computer, Internet or e-mail system, students and staff must accept and adhere to the school E-safety Acceptable Use Policy otherwise they will be logged off.

- Students are provided with an individual network and virtual learning platform username and password. They are expected to change the default password to an individual password of their choice. Access to the Internet, e-mail and all the digital resources at the school is provided for the purposes of educational research and learning. **All students are given their own username, password and protected area of the school network, as well as an e-mail account and access to our Virtual Learning Environment.** They are also provided with information to use these technologies safely and effectively.

- Staff users are provided with a network, virtual learning platform and an Admin/SIMS .net account which also must meet the school's password policy.

- If you think your password has been compromised, it is your sole responsibility to contact ICT Support (ext. 254/222) to arrange for it to be reset. Staff should be mindful that any computer misuse by others on your account will be logged as you and appropriate action taken, which could involve the police.

- Members of staff are aware of their individual responsibilities to protect the security and confidentiality of the school's networks, MIS Systems and Virtual Learning Platforms, including ensuring that passwords are kept safe, not shared and changed periodically. Staff should also make sure that **NO** machines are left unattended while they are logged on, especially when SIMS .net is active for registration.

- When logging on or during registration staff are aware that they should not have the screen projected for all to see, this can lead to passwords being compromised as well as data protection issues.

7 Data Security

Accessing school data is something the school takes very seriously as we are bound legally by the Data Protection Act when dealing with school data. Members of staff must use personal information in line with the principles of the Data Protection Acts. Such data must:

- Be used fairly and lawfully
- Be used for limited, specifically stated purposes
- Be used in a way that is adequate, relevant and not excessive
- Be accurate
- Be kept for no longer than is absolutely necessary
- Be handled according to people's data protection rights
- Be kept safe and secure
- Not be transferred outside the UK without adequate protection.

Members of staff should be aware of their individual responsibilities to protect the security and confidentiality of the school's networks, MIS systems and Virtual Learning Platforms, including ensuring that passwords are kept safe, not shared and changed periodically. Staff should also make sure that **NO** machines are left unattended while they are logged on, especially when Sims .net is active for registration

All important data is backed up on a daily basis, but if any files are accidentally deleted then you must notify the Network Manager or a member of his team as soon as possible on ext. 254/222.

Staff are aware of their responsibilities when accessing school data. They must not;

- Take copies of data held on the admin network unless on school commissioned secured pen drives
- Allow others to view the data
- Edit data unless authorised to do so
- Delete data from the admin network unless authorised to do so
- Use any other USB pen drive other than the encrypted one provided by the school
- Use school related data containing student or staff personal details on their home computers

Sensitive Information and Confidentiality

Information held relating to the work of the school is a resource belonging to the school. This applies whether information is held manually or electronically.

It is expected that all employees and workers will use sensitive information properly and have due respect for confidentiality. If you have access to such information, you should ensure that you:

- Know what information the school treats as confidential (check with your manager if you are unsure)
- Know who is entitled to have access to what information (check with your manager if you are unsure) are responsible and professional in using and allowing access to personal information on students, parents, staff, governors and any others

Confidentiality requirements apply whether relevant data is held manually or electronically.

8 Managing Internet Access

At Enfield County we understand that the Internet is a great resource for teaching and learning. Anyone can view information, send messages, discuss ideas and publish material, which is an invaluable resource to education, but we must identify the risks to young and vulnerable people. All school Internet activity is logged and can be monitored by both the school and LA. These records can be made accessible to relevant authorities such as the police, when required.

The School will take all reasonable precautions to prevent access to inappropriate material. However, due to the international scale and linked nature of Internet content, it is not always possible to guarantee that unsuitable material will never appear on a computer connected to the school network. Neither the school nor Enfield Council can accept liability for any material accessed, or any consequences of Internet access.

- Students will have supervised Internet access to planned teaching material/resources via the schools fixed and mobile technologies.
- Staff will plan and preview any websites before use.
- All users must observe copyright at all times and not distribute any school software or data and must not actively download material or software from the Internet.
- Any homework set that requires the students to access the Internet for research should be checked and monitored by the parent. Parents are advised of this and sent regular E-safety flyers.

9 Virtual Learning Environment (VLE)

Enfield County School uses a Virtual Learning Environment (VLE), Firefly.

- This is a closed environment, requiring teachers and students to log in to use the service.
- The VLE allows teachers to provide materials to support lessons for use both inside and outside the school. Students will be able to hand in work, work collaboratively, ask for help and participate in discussion forums.
- Links will be made to other sites on the Internet. While every care is taken to ensure the direct link is to a suitable site or resource, we can have no control over other links that are made on that site.
- All use of discussion forums and collaborative features are monitored by the teachers that create the resource and all usage can be tracked by the administrator.
- There will be occasions when the student is required to use the VLE as part of a course.

10 Social Media Safeguards

The use of any social media incorporating the Enfield County name requires the official authorisation of the Headteacher.

Use of Twitter by ECS:

- ECS uses Twitter to broadcast important whole school messages and updates.
- All ECS tweets are authorised by a member of the SLT
- Students and parents may 'follow' the ECS feed. ECS will never 'follow' a student or parent
- Any mention/retweets of ECS feed by Twitter followers is visible to ECS
- The Twitter feed is not to be used for Direct Messaging or conversations
- Any abusive/threatening messages sent by a Twitter user will result in the account being blocked and reported.

11 Managing Emerging Technologies (Web 2.0)

Web 2.0/Social networking sites offer users a great, easy to use, creative and mostly free platform to interact with others or the application. However, it is important to recognise that there are issues regarding the appropriateness of some content, contact and culture. We encourage our students to think carefully both in school and at home about the way that information can be added and removed by all users, including themselves.

- Our school website has a separate home page for E-safety and a range of materials are available for viewing/downloading for parents/carers and students. These documents link directly to CEOPS and Childnet so users can receive the most up-to-date material in relation to any E-safety issue.

- All students and staff are advised to be cautious about information they upload and information given by others. Information given by others may be misleading and not from whom they say they are.

- Students are taught not to display images of themselves or others from school and should not display any content that some other individual could use i.e. full name, address, mobile phone number etc. Once an image is placed online it is very difficult to be removed.

- We tell students only to use profiles that are private to them and to deny access to unknown individuals.

- Any incidents of bullying must be reported to the school. We keep all identity and information given confidential and deal with student incidents with reference to the Enfield County School Behaviour Policy.

- Staff may only create blogs, wikis or other Web 2.0 spaces in order to communicate with students using the schools Virtual Learning Platform or other systems approved by the Headteacher or Governors.

- Students should report any online abuse to a trusted adult, usually their Head of Year or KS Co-ordinator who will then inform the Designated Safeguarding Lead or DSL Deputy.

12 Managing E-mail Communication

At Enfield County we use e-mail as a way of communicating with employees. This is the preferred and agreed use of communication in school. School e-mail should not be considered private as all e-mail communications to and from school are monitored for various violations of school policy. (Please refer to the Code of Conduct Policy under the heading e-mail and internet usage for further clarity).

E-mail offers significant benefits to staff and students especially when working on school based projects. In order to meet ICT curriculum requirements in school, students must have experienced sending and receiving e-mails.

- All staff and students in school are given their own unique e-mail address for school business only, this gives us the ability to audit e-mails in a secure manner.
- It is the responsibility of each e-mail account holder to keep their password secure. For the safety of all users, e-mail communications are filtered by MailProtect and logged. Reports are carried out on a regular basis.
- Staff should not contact students or parents or conduct any school business using a personal e-mail address.
- Students should only use e-mail for educational purposes under supervision from a teacher.
- If one of our staff or students receives an e-mail that we consider is particularly disturbing or breaks the law, we will contact the police.
- Any abuse of the e-mail system/policy witnessed by staff or students should be reported to one of the DSLs.
- All e-mail users must adhere to the schools E-safety policy and are reminded that they have accepted both a computer AUP and an Internet/E-mail policy signed by their parents. The use of explicit language and content is strictly prohibited and any violations of this rule will be dealt with by the appropriate school policy.
- Students are taught how to use e-mail safely as part of the ICT curriculum.
- Students must not reveal their personal details or those of others without specific permission from the Headteacher.

13 Mobile Technologies

Many emerging technologies offer new opportunities for teaching and learning including a move towards personalised learning and 1:1 device ownership for children and young people. Many existing mobile technologies such as PDAs, portable media players, gaming devices, mobile and smart phones are familiar to children outside of school too. They often provide a collaborative, well-known device with possible internet access which can open up risk and misuse associated with communication and internet use. All emerging technologies that the school intends to use will be thoroughly examined and tested before implementation in the classroom. We choose to manage the use of the devices in the following ways so that users exploit them appropriately.

- The school allows staff to bring in personal mobile phones and devices for their own use. Under no circumstances does the school allow a member of staff to contact a pupil or parent/carer using their personal device.

- Students are not allowed to use their mobile phone in school, unless directed to do so by a member of staff.

- The sending of inappropriate text, image and video messages between any member of the school community is not allowed.

- Under no circumstances must content created on a mobile device that contains reference to the school or images of any member of the school community be uploaded by a student to any website that shares information i.e. Facebook, MySpace or YouTube. The only exception, with permission, is to the school's Virtual Learning Environment (VLE).

- Students are not able to join their devices to the school network. Therefore, any access to the Internet using these devices will not be filtered by the school.

14 Safe Use of Images

Publishing Students' Images and Work
Traditionally schools have photographed students for a number of reasons: for the school brochure, for school records, as a form or year group, when performing in a sporting activity or drama production and when taking part in a school activity or visit. These photos are then used for displays or can be published as part of the news or twitter feed on the school website. At Enfield County we also use photos to provide a record of all the extra-curricular activities enjoyed during the academic year. These are included in an end of year PowerPoint presentation which is shown at both sites in the last school assembly of the year.

In line with the best practice in safeguarding children and young people Enfield County are careful to ensure that photos of students are published, in such a way that they cannot be accessed by people outside the school and students are not named and cannot be identified. The only exception to this would be if a student was singled out to have a specific achievement recorded in the local press or on the website. Obviously parents and carers would be fully involved in such an event and specific permission sought.

On occasions we do need to film students, for example PE assessments or sharing events on a skiing visit with family back home. Clips are posted on Firefly, our school Virtual Learning Environment, which is assessed via the website and is password protected. However, in order to be able to upload clips onto Firefly they need to be posted on 'You Tube' first. We are therefore careful to anonymise these clips so that neither the students nor the school can be 'googled' and identified. If film clips of student activities are posted on the school website (twitter feed) we ensure that safeguards are in place and that individual students cannot be identified.

Opting Out
At Enfield County, we give parents/carers the opportunity to opt out of publishing their daughter's image or work on the sites listed above and there is a letter on our website for parents/carers to fill in and return to the appropriate department should they wish to opt out.
Student names, e-mail, postal address and mobile numbers will not be published against any image.

Storage of Images
- Images of students and staff are stored securely on the school's network.
- Students and staff are not permitted to use personal portable media for storage of images without express permission from the Headteacher.
- Access to these images are only for the school's staff and students for school purposes only and use on the school's website and VLE.
- Our Network Manager is responsible for the deletion of images no longer in use by the school.

CCTV / Webcams
- The school has CCTV in operation for the safety and security of all persons on the site. The only people that have access to CCTV real-time viewing are SLT, the site management team and reception.
- Any CCTV footage that is captured for security purposes is only available for viewing by the Headteacher, School Business Manager, Site Manager and the Police.
- Webcams are only used in school as learning resources within ICT lessons.

15 Misuse and Infringements

Complaints relating to E-safety should be made to the Designated Safeguarding Lead or one of the Designated Safeguarding Officers. Incidents should be logged.

Handling E-safety Complaints
All users are aware of the procedures for reporting accidental access to inappropriate materials. The breach must be reported immediately to one of the Designated Safeguarding Officers and action taken in line with the Enfield Local Authority Safeguarding Children Board E-safety policy.

Deliberate access to inappropriate material by any user will lead to the incident being logged by one of the DSOs, depending on the seriousness of the offence: investigation by the Headteacher/LA, immediate suspension, possibly leading to dismissal and involvement of the police for very serious offences.

Any staff misuse that suggests a crime has been committed, a child has been harmed or that a member of staff is unsuitable to work with children should be reported to the Local Authority Designated Officer (LADO) within one working day in accordance with the Enfield LA Safeguarding Board Policy.

Any complainant about staff misuse must be referred to the Headteacher and if the misuse is by the Headteacher it must be referred to the Chair of Governors in line with the Enfield Safeguarding Board Child Protection procedures.

16 Acceptable Use Policy: Staff Agreement Form

If malicious or threatening comments are posted on an Internet site about a student or a member of staff:

1. Secure and preserve any evidence.
2. Inform one of the Designated Safeguarding Officers (DSOs), Ms J Scott, Ms K Robbins, Mrs C Egleton, Mrs L Hayden, or Ms P Rutherford (Headteacher)
3. Inform and request that comments be removed if the site is administered externally.
4. The DSO will send all the evidence to Child Exploitation and Online Protection (**CEOP**) Centre at ww.ceop.gov.uk/contact_us.html
5. The DSO will assist in tracing the origin and will inform the Safer Schools Officer as appropriate.

If you are concerned that a child's safety is at risk because you suspect someone is using communication technologies (such as social networking sites) to make inappropriate contact with the child.

1. Report to and discuss with one of the named DSOs in school (see list above). The DSL will contact parents.
2. In consultation with the DSL advise the child on how to terminate the communication and save all evidence.
3. The DSL will contact CEOP http://www.ceop.gov.uk/ and consider the involvement of police and social services.
4. The DSL will inform the Local Authority Designated Officer (LADO).
5. The DSL will consider delivering a parent workshop for the school community.

All of the above incidences must be reported immediately to one of the Designated Safeguarding Officers.

Students should be confident in a no-blame culture when it comes to reporting inappropriate incidents involving the internet or mobile technology: they must be able to do this without fear.

As outlined in the code of conduct policy, we acknowledge that it is important for employees to understand that their own behaviour and the manner in which they conduct themselves with their colleagues, students, parents and other stakeholders sets an example and affects the school environment.

The use of the school communications systems and equipment, including electronic e-mail and Internet/Intranet systems, along with their associated hardware and software, are for official and authorised purposes only. However, we realise that the school communication systems may need to be used for other purposes in relation to our roles and therefore we need to be aware of and commit to the following guidelines:

- I will only use the school's E-mail / Internet / Intranet for purposes in a way that it will not interfere with the performance of my professional duties and will be of reasonable duration and frequency as deemed 'reasonable' by the Headteacher and Governing Body.
- In using the school's E-mail/Internet/Intranet for professional purposes I will always use appropriate written language and not discriminate against, harass or victimise anyone I come into contact with, on any grounds, including: race, ethnic or national origin, gender, sexual orientation, marital status, religious or other beliefs, disability, HIV status, age, trade union involvement, having responsibilities for dependants, working on a temporary or part time basis (note that discrimination, harassment and victimisation include the use of language, making remarks, telling jokes, displaying materials or behaving in a way that may be interpreted as discriminatory, even if not directed at a particular individual(s).

- I will only use the approved, secure e-mail system(s) for legitimate school interest such as enhancing professional interests or education.
- I will not overburden the system or create any additional expense to the school.
- I will conduct myself honestly and appropriately on the Internet, and respect the copyrights, software licensing rules, property rights, privacy and prerogative of others. The transmitting or downloading of materials that are obscene, pornographic, threatening, violently extremist, racially or sexually harassing or in any way contravene the Equal Opportunities Policy is prohibited. I understand that Chat Rooms may not be visited nor any sites known to contain offensive material.
- I will not keep a personal diary or blog on the Internet (whether at school or at home) where reference is made to the school without authorisation. This is not advisable as such usage could cause harm to the reputation of the school and may undermine the confidence of our parent/carers.
- I will report any accidental access to inappropriate materials to the appropriate line manager.
- I will not download any software or resources from the Internet that can compromise the network, or is not adequately licensed.
- I will ensure all documents are saved, accessed and deleted in accordance with the school's network security and confidentiality protocols.
- I will not download or install any software or resources from the Internet on to my PC or laptop without checking with the Network Manager first that it is adequately licenced and compatible with Enfield County's setup.
- I will only use the designated school camera for recording school events and visits.
- I will not transfer images from school visits or events of students or colleagues to another system without permission from the school's visit coordinator.
- I will not take images of students with a personal digital camera without written permission from the Headteacher.
- I will not take images of students with a personal camera phone.
- I will ensure I am aware of digital safeguarding issues so they are appropriately embedded in my classroom practice.
- I will not allow unauthorised individuals to access my E-mail / Internet / Intranet.
- I understand that all Internet usage will be logged and this information could be made available to my manager on request.
- I will only use LA systems in accordance with any corporate policies.
- I understand that this policy is binding to all school staff and that it applies to those staff deployed within the school who are employed by external Agencies or the Council and I will adhere to its principles. I understand that Breaches of the Policy and standards expressed in it could result in disciplinary action, including dismissal for serious offences.

I agree to the terms outlined in the AUP:

Name: (CAPS)

Signature:

Date:

17 Equal Opportunities

Students with Additional Needs

The school endeavours to create a consistent message with parents for all students and this in turn should aid establishment and future development of the schools' E-safety rules.

However, staff are aware that some students may require additional teaching including reminders, prompts and further explanation to reinforce their existing knowledge and understanding of E-safety issues. Therefore, careful consideration is given to group interactions when raising awareness of E-safety.

18 Parental Involvement

Parental involvement is always welcomed at Enfield County School and we consider ourselves to have a good working and professional relationship with the parents of our students. We always try to encourage parents to have their say on any matter related to the school.

Parents/Carers and students are actively encouraged to comment and contribute to adjustments or reviews of the schools E-safety policy by e-mailing ecsgeneral@enfieldcs.enfield.sch.uk

Parents/Carers are asked to read through and sign any acceptable use agreements on behalf of the child on admission to school and any annual Internet/E-mail agreement forms.

Parents/Carers are required to make a decision as to whether they consent to images of their child being taken/used in the public domain. An opt-out letter explaining in detail the use of images is available on the school website.

The school disseminates information to parents relating to E-safety where appropriate in the form of:

- Information Evenings
- Posters
- Website
- Newsletter Items