The Ursuline Preparatory School Ilford

E-Safety Policy

(June 2017)

To live and learn in harmony,
Caring for each other;
Treating everybody as a sister and a brother;
Reflecting Christ's actions and His message too,
By striving for excellence in all that we do

SCHOOL POLICY FOR e-SAFETY

Person responsible: Head teacher and all staff

Date Adopted: March 2007
Policy updated: June 2017

Policy to be reviewed every year

CONTEXT

1. Learning through technology

The Ursuline Preparatory School recognises the internet and other digital technologies provide a vast opportunity for children and young people to learn. Unlike any other mode of technology, the internet and digital technologies allow all those involved in the education of children and young people to promote creativity, stimulate awareness and enhance learning.

As part of our commitment to learning and achievement we want to ensure that the internet and other digital technologies are used to:

- Raise educational standards and promote pupil achievement.
- Develop the curriculum and make learning exciting and purposeful.
- Enable pupils to gain access to a wide span of knowledge in a way that ensures their safety and security.

To enable this to happen we have taken a whole school approach to
E-safety which includes the development of policies and practices, the education and training of staff and pupils and the effective use of the School's infrastructure and technologies.

The school holds steadfastly to the ethos that there should be an equitable learning experience for all pupils using technology. We recognise that technology can allow disabled pupils increased access to the curriculum and other aspects related to learning.

The school is committed to ensuring that all its pupils will be able to use existing, as well as up and coming technologies safely. We are also committed to ensuring that all those who work with children and young people, as well as their parents, are educated as to the dangers that exist so that they can take an active part in safeguarding them.

The nominated senior person for the implementation of the School's E- safety policy is the Head Teacher.

2. Scope of Policy

The policy applies to: all pupils; all teaching and support staff (including peripatetic),school governors and volunteers; all aspects of the School's facilities where they are used by voluntary, statutory or community organizations.

The school will ensure that the following elements are in place as part of its safeguarding responsibilities to pupils:

- a list of authorised persons who have various responsibilities for E-safety;
- a range of policies including acceptable use of policies that are frequently reviewed and updated;
- information to parents that highlights safe practice for children and young people when using the internet and other digital technologies;
- adequate training for staff and volunteers;
- adequate supervision of pupils when using the internet and digital technologies;
- education that is aimed at ensuring safe use of internet and digital technologies;
- a reporting procedure for abuse and misuse.

3. Policies and Procedures

A. The school understands that effective policies and procedures are the backbone to developing a whole-school approach to E-safety. The policies that exist at the school are aimed at providing a balance between exploring the educational potential of new technologies and providing safeguards to pupils.

B. Use of internet facilities, mobile and digital technologies. The school will seek to ensure that internet, mobile and digital technologies are used effectively for their intended educational purpose, without infringing legal requirements or creating unnecessary risk.

C. The school expects all staff and pupils to use the internet, mobile and digital technologies responsibly and strictly according to the conditions below.

These expectations are also applicable to any voluntary and community organizations that makes use of the school's ICT facilities and digital technologies.

Users shall not:
Visit internet sites, make, post, download, upload or pass on, material, remarks, proposals or comments that contain or relate to:
i)Indecent images of children
ii)Promoting discrimination of any kind
iii)Promoting racial or religious hatred
iv)Promoting illegal acts
v)Any other information which may be offensive to peers or colleagues.

D. The school recognises that in certain planned curricular activities, access to otherwise deemed inappropriate sites may be beneficial for educational use. In such circumstances, there is an expectation that access is pre-planned and recorded so that it can be justified if required.

E. Incidents which appear to involve deliberate access to websites, newsgroups and online groups that contain the following material will be reported to the Police:
Images of child abuse (images of children whether they are digital or cartoons, apparently under 16 years old, involved in sexual activity or posed to be sexually provocative)
Adult material that potentially breaches the Obscene Publications Act in the UK
Criminally racist or anti-religious material
Violence and bomb making

Illegal taking or promotion of drugs
Software piracy
Other criminal activity

F. In addition, users may not:
Use the broadband provider's facilities for running a private business;
Enter into any personal transaction that involves the school or associated partners in any way;
Visit sites that might be defamatory or incur liability on the part of the school or associated partners or adversely impact on the image of the school or associated partners;
Upload, download, or otherwise transmit (make, produce or distribute) commercial software or any copyrighted materials belonging to third parties;
Reveal or publicise confidential or proprietary information, which includes but is not limited to: financial information, personal information, databases and the information contained therein, computer/network access codes, and business relationships;
Intentionally interfere with the normal operation of the Internet connection, including the propagation of computer viruses and sustained high volume network traffic (sending or receiving of large files or sending and receiving of large numbers of small files or any activity that causes network congestion) that substantially hinders others in their use of the Internet;
Use the Internet for soliciting, representing personal opinions or revealing confidential information or in any other way that could reasonably be considered inappropriate.
Transmit unsolicited commercial or advertising material either to other user organisations or to organisations connected to other networks, save where the material is embedded within, or is otherwise part of, a service to which the member of the user organisation has chosen to subscribe.
Assist with unauthorized access to facilities or services;
Undertake activities with any of the following characteristics:

wasting staff effort or networked resources, including time on end systems accessible via the network and the effort of staff involved in support of those systems;
corrupting or destroying other users' data; violating the privacy of other users;
disrupting the work of other users;
using the network in a way that denies service to other users (for example, deliberate or reckless overloading of access links or of switching equipment);
continuing to use an item of networking software or hardware after request that use cease because it is causing disruption to the correct functioning of the network;other misuse of the network, such as introduction of viruses.
Use mobile technologies (e.g. 4G, 3G or mobile internet services) in any way to intimidate, threaten or cause harm to others.
Moreover, mobile technologies should not be used to access inappropriate materials or encourage activities that are dangerous or illegal.

Reporting Abuse

The following outlines what to do if a child or adult receives an abusive message or accidentally accesses a website that contains abusive material:
The abusive material should be stored, screenshot if possible and a copy sent to the headteacher of the school. The address (e.g. URL or email) linked to the abuse should also be recorded. However, the screen displaying the abusive material should be hidden from view and/or closed down as soon as possible to avoid further offence. The E-safety Incident/Concern Form should be filled out alongside this and given to the headteacher as soon as possible.

4. Education and Training

The Ursuline Prep School Ilford recognise that the internet and other digital technologies can transform learning; help to improve outcomes for children and young people; promote creativity; all of which add up to a more exciting and challenging classroom experience.
As part of achieving this, we want to create within each school an accessible system, with information and services online, which support personalised learning and choice. However, we realise that it will be necessary for our pupils to have the skills of critical awareness, digital literacy and good online citizenship to enable them to use the internet and other digital technologies safely.
To this end, The Ursuline Prep School Ilford will:-

Enable all pupils to exercise the skills of critical awareness, digital literacy and good online citizenship as part of the school curriculum.

Educate school staff so that they are equipped to support pupils in gaining positive experiences when online and can help pupils develop strategies if they encounter a problem.

Support parents in gaining an appreciation of E-safety for their children and provide them with relevant information on the policies and procedures that govern the use of internet and other digital technologies within the school.

5. Infrastructure and Technology

Partnership working

The Ursuline Prep School recognise that as part of its safeguarding responsibilities there is a need to work in partnership. One of our major partners is the network and broadband supplier. As part of our commitment to partnership working, we fully support and will continue to work with our providers to ensure that pupil and staff usage of the internet and digital technologies is safe.
The Ursuline Prep School Ilford will, as part of its wider safeguarding responsibilities, seek to ensure that voluntary, statutory and community organisation take an approach to their activities that see the welfare of the child as paramount. To this end, we expect any organisation using the school's ICT or digital technologies to have appropriate policies and procedures that are aimed at safeguarding children and young people and reporting concerns.

6. Standards and Inspection

The Ursuline Prep School Ilford recognise the need to have regular inspections of policies and procedures in order to ensure that its practices are effective and that the risks to pupils are minimised.

6.1 Monitoring

Monitoring the safe use of the internet and other digital technologies goes beyond the personal use of the internet and electronic mail a pupil or member of staff may have, The Ursuline Prep School Ilford recognise that in order to develop an effective whole school E-safety approach there is a need to monitor patterns and trends of use inside school and outside school (Education and Inspections Act 2006, Section 89(5)).
With regard to monitoring trends, within the school and individual use by school staff and pupils, The Ursuline Prep School ilford will audit the use of the internet and electronic mail in order to ensure compliance with this policy. The school will also work with its internet service provider to further ensure compliance.
Another aspect of monitoring, which our school will employ, is the use of mobile technologies by pupils, particularly where these technologies may be used to cause harm to others, e.g. bullying (see anti-bullying policy for further information). We will also ensure that school staff understand the need to monitor our pupils, and where necessary, support individual pupils where they have been deliberately or inadvertently been subject to harm.

6.2 Sanctions

The Ursuline Prep School Ilford has been careful to develop in conjunction with its partners, policies and procedures to support the innocent in the event of a policy breach and enable the School to manage such situations in, and with, confidence. Where there is inappropriate or illegal use of the internet and digital technologies, the following sanctions will be applied:

Child / Young Person

The child/young person will be disciplined according to the behaviour policy of the school, which could ultimately include the use of internet and digital technologies being withdrawn.

Serious breaches may lead to the incident being reported to the Police or other regulatory bodies, for instance, illegal Internet use or child protection concerns.

Adult (Staff and Volunteers)

The adult may be subject to the disciplinary process, if it is deemed he/she has breached the policy

Serious breaches may lead to the incident being reported to the Police or other regulatory bodies, for instance, illegal Internet use or child protection concerns.

If inappropriate material is accessed, users are required to immediately report this to the headteacher so this can be taken into account for monitoring purposes.

7. Working in Partnership with Parents and Carers

The Ursuline Prep School Ilford are committed to working in partnership with parents and carers and understand the key role they play in the Esafety of their children, through promoting E- safety at home and elsewhere.

The Ursuline Prep School Ilford also appreciates that there may be some parents and carers who are concerned about the use of the internet, email and other digital technologies in school. In such circumstances school staff will meet with parents and carers to discuss their concerns and agree upon a series of alternatives that will allow their child to fully access the curriculum, whilst remaining safe.

8. Appendices of the E-safety Policy

There are multiple aspects of the school's E-safety policy, which include acceptable use policies for both staff and pupils; ICT equipment (onsite and offsite); data security and retention. The various policy documents relating to these aspects of the school's E-safety policy can be obtained from the headteacher for scrutiny, if required.

The Technologies

ICT in the 21st Century has an all-encompassing role within the lives of children and adults. New technologies are enhancing communication and the sharing of information. Current and emerging technologies used in school and, more importantly in many cases, used outside of school by children include:

- The Internet
- E-mail
- Instant messaging http://www.msn.com, http://info.aol.co.uk/aim/) often using simple web cams
- Blogs (an on-line interactive diary)
- Podcasting (radio/audio broadcasts downloaded to computer or MP3/4 player)
- Social networking sites (popular www.myspace.com, www.piczo.com, www.bebo.com, http://www.hi5.com)
- Video broadcasting sites (popular http://www.outube.com)
- Chat rooms (popular www.teenchat.com, www.habbohotel.co.uk)
- Gaming sites (popular www.neopets.com, http://www.miniclip.com/games/en/, http://www.runescape.com/)
- Music download sites (popular http://www.apple.com/itunes, http://www.napster.co.uk, http://www.kazzaa.com, http://www.livewire.com)
- Mobile phones with camera and video functionality
- Smart phones with e-mail, web functionality and cut down 'office' applications

Whole School Approach to the Safe Use of ICT

Creating a safe ICT learning environment includes three main elements at this school:

- An effective range of technological tools
- Policies and procedures, with clear roles and responsibilities
- A comprehensive e-Safety education programme for pupils, staff and parents

Roles and Responsibilities

e-Safety is recognized as an essential aspect of strategic leadership in this school and the Head, with the support of Governors, aims to embed safe practices into the culture of the school. The head teacher ensures that the Policy is implemented and compliance with the Policy monitored. The responsibility for e-Safety has been designated to a member of the senior management team.

Our school **e-Safety Co-ordinator** is Mrs. Victoria MacNaughton
Our e-Safety Co-ordinator ensures they keep up to date with e-Safety issues and guidance through liaison with the Local Authority, and through organizations such as Becta and The Child Exploitation and Online Protection (CEOP). The school's e-Safety co-ordinator ensures the Head, Senior Management Team and Governors are updated as necessary.

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

All teachers are responsible for promoting and supporting safe behaviours in their classrooms and following school e-Safety procedures. Central to this is fostering a 'No Blame' culture so pupils feel able to report any bullying, abuse or inappropriate materials.

All staff should be familiar with the schools' Policy including:

- Safe use of e-mail

- Safe use of internet including use of internet-based communication services such as instant messaging and social network
- 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 pupil information/photographs and use of website
- e-Bullying/Cyber-bullying procedures
- Their role in providing e-Safety education for pupils

Staff are reminded/updated about e-Safety matters at least once a year.

How will complaints regarding e-Safety be handled?

The school will take all reasonable precautions to ensure e-Safety. However, owing to the international scale and linked nature of Internet content, the availability of mobile technologies and speed of change, it is not possible to guarantee that unsuitable material will never appear on a school computer or mobile device. The school cannot accept liability for material accessed, or any consequences of Internet access.

Staff and pupils are given information about infringements in use and possible sanctions. Sanctions available include:

- Interview/counseling by e-Safety Co-ordinator/Head teacher
- Informing parents or carers
- Removal of Internet or computer access for a period, (which could ultimately prevent access to files held on the system)
- Referral to Police

Our e-Safety Co-ordinator acts as first point of contact for any complaint. Any complaint about staff misuse is referred to the Head Teacher.

Complaints of cyber-bullying are dealt with in accordance with our Anti-Bullying Policy.

Complaints related to child protection are dealt with in accordance with school child protection procedures.

KEEPING SAFE: STOP, THINK, BEFORE YOU CLICK!

12 RULES FOR RESPONSIBLE ICT USE

These rules will keep everyone safe and help us to be fair to others.

- I will only use the school's computers for schoolwork and homework
- I will only delete my own files
- I will not look at other people's files without their permission
- I will keep my login and password secret
- I will not bring files into school without permission
- I will ask permission from a member of staff before using the Internet and will not visit Internet sites I know to be banned by the school
- I will only e-mail people I know, or my teacher has approved
- The messages I send, or information I upload, will always be polite and sensible
- I will not open an attachment, or download a file, unless I have permission or I know and trust the person who has sent it
- I will not give my home address, phone number, send a photograph or video, or give any other personal information that could be used to identify me, my family or my friends, unless my teacher has given permission
- I will never arrange to meet someone I have only ever previously met on the Internet or by email or in a chat room, unless my parent, guardian or teacher has given me permission and I take a responsible adult with me
- If I see anything I am unhappy with or I receive a message I do not like, I will not respond to it but I will tell a teacher/responsible adult

PUPIL e-SAFETY AGREEMENT FORM

KEEPING SAFE: STOP, THINK, BEFORE YOU CLICK

Pupil name: _____

I have read the school 'rules for responsible ICT use'. My teacher has explained them to me.

I understand these rules are there to help keep me safe, and my friends and family safe. I agree to follow the rules.

This means I will use the computers, Internet, e-mail, online communities, digital cameras, video recorders, and other ICT in a safe and responsible way. I understand that the school can check my computer files and the Internet sites I visit, and that if they have concerns about my safety, that they may contact my parent/guardian.

Pupil's signature: _____

Date: _____

e-SAFETY AGREEMENT FORM: PARENTS

Parent/Guardian name: _____

Pupil name (s): _____

As the parent or legal guardian of the above pupil(s), I grant permission for my daughter to have access to use the Internet, school e-mail and other ICT facilities at school.

I know that my daughter has signed an e-safety agreement form and that they have a copy of the 12 'rules for responsible ICT use'.

I accept that ultimately the school cannot be held responsible for the nature and content of the materials accessed through the Internet and mobile technologies, but I understand that the school will take every reasonable precaution to keep pupils safe and to prevent pupils from accessing inappropriate materials. These steps include using an educationally filtered service, restricted access e-mail, employing appropriate teaching practice and teaching e-safety skills to pupils.

I understand that the school can check my child's computer files, and the Internet sites they visit, and that if they have concerns about their e-safety or e-behaviour that they will contact me.

I will support the school by promoting safe use of the Internet and digital technology at home and will inform the school if I have any concerns over my child's e-safety.

Parent/guardian signature: _____

Date: _____

Use of digital images – photography and video

I also agree to the school using photographs of my child or including them in video material, as described in the document 'Use of digital images – photography and video'. I have read and understood this document. I understand that images will only be used to support learning activities or in publicity that reasonably promotes the work of the school, and for no other purpose.

Parent/guardian signature: _____

Date: _____

USE OF DIGITAL IMAGES – PHOTOGRAPHY AND VIDEO

To comply with the Data Protection Act 1998, we need your permission before we can photograph or make recordings of your daughter/son.

We follow the following rules for any external use of digital images:

- If the pupil is named, we avoid using their photograph
- If their photograph is used, we avoid naming the pupil

Where showcasing examples of pupils work we only use their first names, rather than their full names.

If showcasing digital video work to an external audience, we take care to ensure that pupils aren't referred to by name on the video, and that pupils' full names aren't given in credits at the end of the film.

Only images of pupils in suitable dress are used.

Staff are not allowed to take photographs or videos on their personal equipment.

Examples of how digital photography and video may be used include:

- Your child being photographed (by the classroom teacher, teaching assistant or another child) as part of a learning activity; e.g. photographing children at work and then sharing the pictures on the interactive whiteboard in the classroom allowing children to see their work and make improvements.
- Your child's image for presentation purposes around the school; e.g. in school wall displays and power point presentations to capture images around the school or in the local area as part of a project or lesson.
- Your child's image being used in a presentation about the school and its work in order to share its good practice and celebrate its achievements, which is shown to other parents, schools or educators; e.g. within a CDROM/DVD or a document sharing good practice; in our school prospectus or on our school website. In rare events, your child could appear in the media if a newspaper photographer or television crew attend an event.

Note: If we, or you, actually wanted your child's image linked to their name we would contact you separately for permission, e.g. if your child won a national competition and wanted to be named in local or government literature.

Further information for parents on e-Safety can be found at:
http://www.parentscentre.gov.uk/usingcomputersandtheinternet/linksbytopic/

Use of digital images – photography and video: I also agree to the school using photographs of my child or including them in video material, as described in the document 'Use of digital images – photography and video'. I have read and understood this document. I understand that images will only be used to support learning activities or in publicity that reasonably promotes the work of the school, and for no other purpose.

Parent/guardian signature: _____

Date: _____

Ilford Ursuline Preparatory School

ICT Acceptable Use Agreement Form

EMAIL / INTERNET / INTRANET / NETWORK USAGE POLICY

- I will only use the school's Email / Internet / Intranet for Professional purposes or for uses deemed 'reasonable' by the Head and Governing Body.
- I will only use the approved, secure email system(s) for any school business
- I will not browse, download or send material that could be considered offensive to colleagues
- 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 use my own personal technological equipment at school without prior permission. I will not connect a computer or laptop to the network / Internet that does not have up-to-date version of anti-virus software
- I will not use personal digital cameras or camera phones for transferring images of pupils or colleagues without permission
- I will ensure I am aware of digital safety-guarding issues so they are appropriately embedded in my classroom practice
- I will not allow unauthorized individuals to access Email / Internet / Intranet
- I understand that all Internet usage will be logged and this information could be made available to my manager on request
- I agree and accept that any computer, laptop or IT equipment loaned to me by the school, is provided solely to support my professional responsibilities and business purposes. I will notify the school of any "significant personal use" as defined by HM Revenue & Customs
- I will only use school systems in accordance with the School Usage Policies
- I understand that failure to comply with the Usage Policy could lead to disciplinary action

User Signature

I agree to abide by the above Acceptable Usage Policy

Signature: _____

Date: _____

Full Name: _____

Job Title: _____

Authorised Signature (Head Teacher)

Is this member of staff temporary? _____

If yes, contract end date: _____

I approve this email account / connection to the Internet / Intranet

Signature: _____

Date: _____

Full Name: _____ (printed)