The Ursuline Preparatory School Ilford

E-Safety Policy

(April 2019)

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: April 2019

Policy to be reviewed every year

Introduction

It is the duty of The Ursuline Preparatory School Ilford to ensure that every pupil in its care is safe; and the same principles apply to the digital world as apply to the real world. IT and online communications provide unrivalled opportunities for enhanced learning in addition to traditional methods, but also pose greater and more subtle risks to young people. Our pupils are therefore taught how to stay safe in the online environment and how to mitigate risks, including but not limited to the risk of identity theft, bullying, harassment, grooming, stalking, abuse and radicalisation.

New technologies are continually enhancing communication, the sharing of information, learning, social interaction and leisure activities. Current and emerging technologies used today include:

- *Websites;*
- *Email and instant messaging;*
- *Blogs;*
- *Social networking sites;*
- *Chat rooms;*
- *Music / video downloads;*
- *Gaming sites;*
- *Text messaging and picture messaging;*
- *Video calls;*
- *Podcasting;*
- *Online communities via games consoles; and*
- *Mobile internet devices such as smart phones and tablets.*

Note: The Ursuline Preparatory School Ilford limits and blocks use of some of these technologies within the school.

This policy, supported by the IT Acceptable Use policy (for all staff, visitors and pupils), is implemented to protect the interests and safety of the whole school community. It aims to provide clear guidance on how to minimise risks and how to deal with any infringements.

It is linked to the following school policies:

- *Safeguarding;*
- *Anti-Bullying;*
- *IT Acceptable Use Policy;*
- *Social Networking Policy;*
- *E-Safety Policy*

Whilst exciting and beneficial both in and out of the context of education, much IT, particularly online resources, are not consistently policed. All users need to be aware of the range of risks associated with the use of these internet technologies.

At The Ursuline Preparatory School Ilford we understand the responsibility to educate our pupils on e-safety issues; teaching them the appropriate behaviours and critical thinking skills necessary to enable them to remain both safe and within the law when using the internet and related technologies in and beyond the classroom. We also understand the importance of involving pupils in discussions about e-safety and listening to their fears and anxieties as well as their thoughts and ideas.

Scope of this Policy

This policy applies to all members of the school community, including staff, pupils, parents and visitors, who have access to and are users of the school IT systems. In this policy 'staff' includes teaching and non-teaching staff, governors, and regular volunteers. 'Parents includes pupils' carers and guardians. 'Visitors' includes anyone else who comes to the school, including occasional volunteers.

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

Roles and responsibilities

Headteacher and the Senior Leadership Team

The Headteacher is responsible for the safety of the members of the school community and this includes responsibility for e-safety. The Headteacher has delegated day-to-day responsibility to the Computing Coordinator.

In particular, the role of the Headteacher and the Senior Leadership team is to ensure that: staff, in particular the IT Co-ordinator are adequately trained about e-safety; and staff

are aware of the school procedures and policies that should be followed in the event of the abuse or suspected breach of e-safety in connection to the school.

E-safety

The School's Computing Co-ordinator and Safeguarding Officer are responsible to the Headteacher for the day to day issues relating to e-safety. They will keep up to date on current e-safety issues and guidance issued by relevant organisations, including the ISI, the Local Authority, CEOP (Child Exploitation and Online Protection), Childnet International and the Local Authority Safeguarding Children Board.

IT staff

The school's technical staff have a key role in maintaining a safe technical infrastructure at the school and in keeping abreast with the rapid succession of technical developments. They are responsible for the security of the school's hardware system, its data and for training the school's teaching and administrative staff in the use of IT. They monitor the use of the internet and emails, maintain content filters, and will report inappropriate usage to the Computing Co-ordinator.

Teaching and support staff

All staff are required to sign the IT Acceptable Use Policy before accessing the school's systems.

As with all issues of safety at this school, staff are encouraged to create a talking and listening culture in order to address any e-safety issues which may arise in classrooms on a daily basis.

Pupils

Pupils are responsible for using the school IT systems in accordance with the IT Acceptable Use Policy, and for letting staff know if they see IT systems being misused.

Parents and carers

The Ursuline Preparatory School Ilford believes that it is essential for parents to be fully involved with promoting e-safety both in and outside of school. We regularly consult and discuss e-safety with parents and seek to promote a wide understanding of the benefits and risks related to internet usage.

Outside agencies attend the school on an annual basis to provide information and training for parents.

The school will always contact parents if it has any concerns about pupils' behaviour in this area and likewise it hopes that parents will feel able to share any concerns with the school.

Parents and carers are responsible for endorsing the school's IT Acceptable Use Policy.

Education and training

Staff: awareness and training

New staff receive information on The Ursuline Preparatory School Ilford's e-Safety and IT Acceptable Use policies as part of their induction. All staff receive regular information and training on e-safety issues in the form of INSET training and internal meeting time, and are made aware of their individual responsibilities relating to the safeguarding of children within the context of e-safety.

All staff working with children are responsible for demonstrating, promoting and supporting safe behaviours in their classrooms and following school E-Safety procedures. These behaviours are summarised in the IT Acceptable Use Policy which must be signed and returned before use of technologies in school. Teaching staff are encouraged to incorporate e-safety activities and awareness within their subject areas and through a culture of talking about issues as they arise. They should know what to do in the event of misuse of technology by any member of the school community.

A record of concern must be completed by staff as soon as possible if any incident relating to e-safety occurs and be provided directly to the school's Computing Coordinator and Safeguarding Lead.

Pupils: E-Safety in the curriculum

IT and online resources are used increasingly across the curriculum. We believe it is essential for e-safety guidance to be given to pupils on a regular and meaningful basis. We continually look for new opportunities to promote e-safety and regularly monitor and assess our pupils' understanding of it. The school provides opportunities to teach about e-safety within a range of curriculum areas and IT lessons. Educating pupils on the dangers of technologies that may be encountered outside school will also be carried out via PSHEE, by presentations in assemblies, as well as informally when opportunities arise. The school also arranges outside specialists to speak to pupils on a regular basis.

At age-appropriate levels, pupils are taught about their e-safety responsibilities and to look after their own online safety. Pupils can report concerns to the Safeguarding Lead or the Computing Coordinator or indeed any member of staff at the school.

Pupils are also taught informally about relevant laws applicable to using the internet; such as data protection and intellectual property. Pupils are taught about respecting other people's information and images through discussion and classroom activities.

Pupils should be aware of the impact of cyber-bullying and know how to seek help if they are affected by these issues (see also the school's Anti-bullying Policy, which describes the preventative measures and the procedures that will be followed when the school discovers cases of bullying). Pupils may approach Safeguarding Lead as well as parents, peers and other school staff for advice or help if they experience problems when using the internet and related technologies.

Parents

The school seeks to work closely with parents and guardians in promoting a culture of e-safety. The school will always contact parents if it has any concerns about pupils' behaviour in this area and likewise it hopes that parents will feel able to share any concerns with the school.

The school recognises that not all parents and guardians may feel equipped to protect their child when they use electronic equipment at home. The school therefore arranges

regular discussion meetings for parents when an outside specialist advises about e safety and the practical steps that parents can take to minimise the potential dangers to their children without curbing their natural enthusiasm and curiosity.

Policy Statements

1. Use of school and personal devices

Staff

School devices assigned to a member of staff as part of their role must have a password or device lock so that unauthorised people cannot access the content. When they are not using a device staff should ensure that it is locked to prevent unauthorised access.

Staff at The Ursuline Preparatory School Ilford are permitted to bring in personal devices for their own use. They may use such devices only when children and not present.

Personal telephone numbers, email addresses, or other contact details may not be shared with pupils or parents / carers and under no circumstances may staff contact a pupil or parent / carer using a personal telephone number, email address, social media, or other messaging system, unless specifically permitted by the headteacher for extenuating reasons.

Pupils

No personal devices belonging to pupils are to be used at school, whether for school work or personal use, unless specifically authorised by the headteacher.

2. Use of internet and email

Staff

Staff must not access social networking sites, personal email, which is unconnected with school work or business from school devices or whilst teaching / in front of pupils.

When accessed from staff members' own devices / off school premises, staff must use social networking sites with extreme caution, being aware of the nature of what is published online and its potential impact on their professional position and the reputation of the school. Refer to Social Networking Policy for more details.

The school has taken all reasonable steps to ensure that the school network is safe and secure. Staff should be aware that email communications through the school network and staff email addresses are monitored.

Staff must immediately report to the Computing Coordinator the receipt of any communication that makes them feel uncomfortable, is offensive, discriminatory, threatening or bullying in nature and must not respond to any such communication. Staff must remain alert to the risk of fraudulent emails and should report emails they suspect to be fraudulent to Computing Coordinator.

Any online communications must not either knowingly or recklessly: place a child or young person at risk of harm, or cause actual harm; or bring The Ursuline Preparatory School Ilford into disrepute; or breach confidentiality; or breach copyright; or breach data protection legislation; or do anything that could be considered discriminatory against, or bullying or harassment of, any individual, for example by: making offensive or derogatory comments relating to sex, gender reassignment, race (including nationality), disability, sexual orientation, religion or belief or age; using social media to bully another individual; or posting links to or endorsing material which is discriminatory or offensive.
Under no circumstances should school pupils be added as social network 'friends' or contacted through social media.
Any digital communication between staff and pupils or parents / carers must be professional in tone and content. Under no circumstances may staff contact a pupil or parent / carer using any personal email address. The school ensures that staff have access to their work email address when offsite, for use as necessary on school business.

Pupils
There is strong anti-virus and firewall protection on our network. Spam emails and certain attachments will be blocked automatically by the email system. If this causes problems for school work/research purposes, pupils should contact Computing Coordinator for assistance.

Pupils must not respond to any communication that makes them feel uncomfortable, is offensive, discriminatory, threatening or bullying in nature and should immediately report such a communication, to the Computing Coordinator or any member of staff.

The school expects pupils to think carefully before they post anu information online, or repost or endorse content created by other people. Content posted should not be able to be deemed inappropriate or offensive, or likely to cause embarrassment to the individual or others.

Pupils must report any accidental access to inappropriate content directly to the Computing Coordinator or any member of staff. Deliberate access to any inappropriate materials by a pupil will lead to the incident being recorded on their file and will be dealt with under the school's Behaviour Management Policy. Pupils should be aware that all internet usage via the school's systems and its wifi network is monitored.
Certain websites are automatically blocked by the school's filtering system. If this causes problems for school work/research purposes, pupils should contact the Computing Coordinator for assistance.

3. Data storage and processing

The school takes its compliance with the Data Protection Act 2018 and General Data Protection Regulations (GDPR) seriously. Please refer to the Privacy Notice and the IT Acceptable Use Policy for further details.

Staff and pupils are expected to save all data relating to their work to their school laptop which is synced to the school central server.

Staff may only take information offsite when authorised to do so, and only when it is necessary and required in order to fulfil their role. No personal data of staff or pupils should be stored on personal or school memory sticks.

Any security breaches or attempts, loss of equipment and any unauthorised use or suspected misuse of IT must be immediately reported to the Computing Coordinator.

4. Password security

Staff have individual school network logins and storage folders on the server. Staff are regularly reminded of the need for password security.

All members of staff should: use a strong password (usually containing eight characters or more, and containing upper and lower case letters as well as numbers). not write passwords down; and not share passwords with other pupils or staff.

5. Safe use of digital and video images

The development of digital imaging technologies has created significant benefits to learning, allowing staff and pupils instant use of images that they have recorded themselves or downloaded from the internet. However, staff, parents / carers and pupils need to be aware of the risks associated with publishing digital images on the internet. Such images may provide avenues for cyberbullying, stalking or grooming to take place. Digital images may remain available on the internet forever and may cause harm or embarrassment to individuals in the short or longer term.

When using digital images, staff should inform and educate pupils about the risks associated with the taking, use, sharing, publication and distribution of images. In particular they should recognise the risks attached to publishing their own images on the internet (e.g. on social networking sites).

Parents/carers are welcome to take videos and digital images of their children at school events for their own personal use. To respect everyone's privacy and in some cases protection, these images should not be published on blogs or social networking sites.

Staff and volunteers are allowed to take digital/video images to support educational aims, but must follow this policy and the IT Acceptable Use Policy/IT Policy/EYFS Policy concerning the sharing, distribution and publication of those images. Those images must only be taken on school equipment: personal equipment should not be used for such purposes.

Care should be taken when taking digital/video images that pupils are appropriately dressed and are not participating in activities that might bring the individuals or the school into disrepute. Pupils must not, use, share, publish or distribute images of others. Written permission from parents or carers will be obtained before photographs of students/pupils are published on the school website (see Acceptance Form, Use of Images of pupils by the School form and IT Acceptable Use Policy for more information). Photographs published on the school website, or displayed elsewhere, that include pupils, will be selected carefully

and will comply with good practice guidance on the use of such images. Pupils' full names will not be used with photographs.

6. Misuse

The Ursuline Preparatory School Ilford will not tolerate illegal activities or activities that are inappropriate in a school context, and will report illegal activity to the police and/or the LSCB. If the school discovers that a child or young person is at risk as a consequence of online activity, it may seek assistance from the CEOP.

Incidents of misuse or suspected misuse must be dealt with by staff in accordance with the school's Safeguarding Policy.

The school will impose a range of sanctions on any pupil who misuses technology to bully, harass or abuse another pupil in line with our Anti-Bullying Policy.

7. Complaints

As with all issues of safety at The Ursuline Preparatory School Ilford if a member of staff, a pupil or a parent / carer has a complaint or concern relating to e-safety prompt action will be taken to deal with it. Complaints should be addressed to the Computing Coordinator in the first instance, who will liaise with the Headmistress/management team and undertake an investigation where appropriate. Please see the Complaints Policy for further information.

Incidents of or concerns around e-safety will be recorded using a "Cause for concern" form, found in the Appendices of the Safeguarding and Child Protection Policy; and reported to the school's Computing Coordinator and the Designated Safeguarding Lead, in accordance with the school's Safeguarding and Child Protection Policy.

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: _____

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)