The Ursuline Preparatory School Ilford

E-Safety Policy

(October 2023)

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

Persons responsible: Computing subject co-ordinator and Head Teacher

Date Adopted: ***October 2023***

Date of Policy Review: ***October 2024***

HOW THE POLICY WAS DEVELOPED

The policy was developed and adjusted to be in line with the updated Keeping Children Safe in Education 2023 and its emphasis on online safety.

HOW IT RELATES TO THE SCHOOL DEVELOPMENT PLAN

- *To enhance the quality of Computing by further developing it as a tool across the whole curriculum subject range and also as a stand-alone subject*
- *To ensure that computing equipment enhances learning across the curriculum*
- *To provide training opportunities for ICT to support teachers to deliver curriculum effectively*
- *To enable parents to understand teaching and learning to support their children effectively*

RATIONALE

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.

AIMS AND OBJECTIVES

- *To provide pupils with the computational skills necessary to become independent learners*
- *To promote safe and sensible use of technology through a dedicated e-safety curriculum.*
- *To use new technologies to enable good quality teaching and learning to take place*
- *To ensure appropriate and equal access to technology for all children regardless of age, gender, ethnicity or ability*
- *To ensure our pupils take advantage of the ever quickening pace of technological change*
- *To provide pupils with an understanding of the role technology plays in everyday life at present and its importance in the future*
- *To give children opportunities to access the Computing Curriculum through home-school links.*

LINKS TO OTHER POLICIES

- Safeguarding;
- Anti-Bullying;
- Behaviour Management Policy;
- IT Acceptable Use Policy;
- Social Networking Policy.

The dfe document Keeping Children Safe in Education 2023

Online safety policy: Paragraph 138 This section now includes reference to child protection policies and appropriate filtering and monitoring on school devices and school networks. Child protection policies should include how the school approaches filtering and monitoring on school devices and school networks.
Filtering and monitoring: Paragraph 142 A new section has been added which references the new published filtering and monitoring standards. Governing bodies should refer to these standards to ensure that the school has appropriate/effective filtering and monitoring systems in place.
Information security and access management: Paragraph 144 This now includes a link to the Cyber security standards for schools and colleges

ORGANISATION & PLANNING

To ensure well-developed, broad and consistent lessons, covering all necessary strands of the computing curriculum, we follow the Twinkl scheme of work. This also provides us with a number of cross-curricular links and a clear progression of computing skills across the Key Stages. The planning and software supports our teachers in delivering clear skills using the appropriate and recommended software. It is the role of the Computing Co-ordinator to ensure that plans are reviewed and that key skills are being covered.

EYFS

It is important in the Early Years Foundation Stage to give children a broad, play-based experience of computing in a range of contexts, including outdoor play. Computing is not just about computers. EYFS learning environments should feature computing scenarios based on experience in the real world, such as in role play. Children gain confidence, control and language skills through opportunities to 'paint' on the whiteboard or programme a toy. Recording devices can support children to develop their communication skills. This is particularly useful with children who have English as an additional language.

CROSS-CURRICULAR LINKS

It is the class teacher's responsibility to find links to computing within the wider curriculum for more frequent use within the classroom.

RESOURCES

All resources are available for the use of all members of staff and students. The school acknowledges the need to continually maintain, update and develop its resources to make progress towards a consistent, compatible computing system by investing in resources that will effectively deliver the strands of curriculum and support the teaching and learning of computing across the school. Staff are required to inform the computing technician of any faults as soon as they are noticed. The computing technician will be in school two days a week to ensure the systems are running to a high level and to offer assistance in further developing the school's use of IT. The Headteacher and the Bursar are responsible for the storing and ordering of these resources and can be referred to for help concerning them.

RESPONSIBILITIES

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 Computimg subject 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 the Designated 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 computing technician is 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 Headteacher.

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.

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.

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 technician 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 technician.

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/IT technician 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 any 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 IT technician 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/computer 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 technician.

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). All staff should not write passwords down; and should not share passwords with other pupils or staff. All passwords are issued by the Computer technician.

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/ Computing 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.

ASSESSMENT AND RECORD KEEPING

At The Ursuline Preparatory School Ilford, assessment is an integral part of the teaching process. Assessment is used to inform planning and to facilitate differentiation. The assessment of children's work is on-going to ensure that understanding is being achieved and that progress is being made. Feedback is given to the children as soon as possible. At the end of each unit the pupils will be assessed against the key criteria from the unit and identified as 'working towards', 'meeting' or exceeding the expectations.

FORMAL ASSESSMENT

- *Topic work is used to monitor progress and to identify any gaps within their learning.*
- *Teachers use progression ,frameworks Twinkl Jigsaw progression assessment tool whilst marking to identify strengths and weaknesses and use it to adapt their planning accordingly.*

INFORMAL ASSESSEMENT

This is made by talking to children about their understanding as they work and targeting individual children or groups indicated in our planning.

We use assessment to:-

- *inform our teaching*
- *inform our planning*
- *inform the child*
- *diagnose difficulties*
- *evaluate and compare performance (of child/year groups/National Standards. Analysis completed by senior management team and coordinators)*
- *Ensure we monitor progress*
- *Evaluate our own performance*
- *Report to parents*

EQUAL OPPORTUNITIES

We will try to ensure that:

- *all pupils are able to use the full range of materials and processes regardless of their race, gender or culture, taking into account any appropriate differentiation.*
- *contexts for computing activities should always support the school's policy on Equal Opportunities and incorporate real life opportunities*
- *teachers identify and provide for pupils' special needs*

HEALTH AND SAFETY

Staff are trained to take care of all items and will ensure safe handling of materials and resources.

PARENTAL INVOLVEMENT

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 consult and discuss e-safety with parents and seek to promote a wide understanding of the benefits and risks related to internet usage.

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.

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 has a dedicated E-Safety page on its internet page which is accessible to all, as well as a monthly E-Safety newsletter. This newsletter advises about e safety and the practical steps that parents can take to minimize the potential dangers to their children without curbing their natural enthusiasm and curiosity.

REPORTING

- *Formal interviews with parents are held in the Autumn and Spring terms. Parents are welcome to make an appointment at other times to discuss concerns.*
- *ICT reports are sent to parents in July. Interim reports (short reports) are sent out in April.*