



URSULINE HIGH SCHOOL
Wimbledon

Digital Learning and
Safety Policy

June 2023

ACTING HEADTEACHER MR EOIN KELLY BA (HONS), MSC, PGCE

URSULINE HIGH SCHOOL CRESCENT ROAD WIMBLEDON LONDON SW20 8HA

E-MAIL: enquiries@ursulinehigh.merton.sch.uk

WEBSITE: www.ursulinehigh.merton.sch.uk

“Do something, get moving. Be confident, risk new things, stick with it and then be ready for big surprises!” **St Angela**

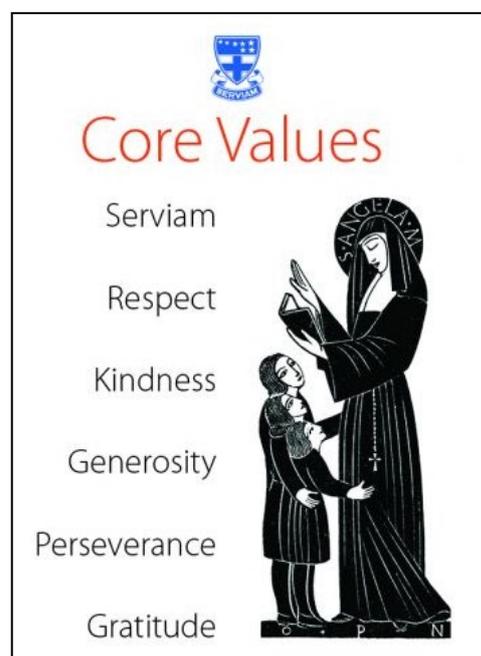
Our Mission

Inspired by the life and work of Saint Angela Merici, our Ursuline school commits itself to education for tomorrow’s world within the dynamic tradition of Catholic belief and practice.

As a Christian community, characterised by a spirit of respect, trust and joy, we promote excellence in every aspect of life, thereby fully developing each individual.

Aims

- Set standards of excellence in teaching and learning and to provide a broad, balanced and relevant curriculum
- Develop personal qualities of understanding of self and others, self-discipline and motivation, responsibility, maturity, creative freedom and integrity
- Foster an attitude of respect for all regardless of age, race, colour, creed or gender
- Build peace, promote justice, social concern and, through the celebration of difference, the equality of all people
- Widen horizons, encourage a sense of commitment and service to the wider world, and to enable each one to go on learning and changing all through life



By the time they leave the Ursuline, our students live out the values of St Angela by:

Being willing in the spirit of Serviam to develop their gifts and talents for the good of others and those most in need.



Being able to recognise the uniqueness of individuals by showing respect and love for all while building a community based on the common good.



Being kind, compassionate, strong and confident women of faith with high aspirations for themselves and others.



Being able to adapt to the sign of the times whilst understanding what really matters in life.



Being able to understand their role in the stewardship of the environment.

At Ursuline High School, we enable our students to be future ready, proficient in the general and specialist skills for learning, life and work with exceptional fluency in the language of a globally connected society.

Our curriculum should be future orientated, globally informed, locally contextualised and centred on well-being at individual, societal and environmental levels.

- ☞ Outstanding curriculum provision must future proof the skills, knowledge and behaviours of our students to meet the changing markets in the next 10-20 years.
- ☞ Ursuline High School is committed to the continued provision of a varied and engaging education, including strong pastoral support, in the event of full or partial school closure. This policy will summarise how this provision will take place, so that there are consistent and well-understood expectations of the level of support that will be provided for all concerned. The intended outcome is to support all pupils, maximise pupil learning and continue to follow the curriculum, whilst allowing opportunities for additional unplanned learning that radical changes to lifestyle and ways of working may present.
- ☞ Ensure compliance with all digital safety procedures.

Using ICT to Transform Learning

We utilise the most up to date technology to engage learners and equip them for the world of further education and employment. Our Digital Learning strategy is based on extensive research and aims to combine all aspects of ICT with the curriculum to ensure that all of our students are proficient in its application. By teaching the five key skills of ICT through the seven key applications of ICT, we are empowering our students to be future ready. The five skills are:

1. Information and data literacy
2. Communication and collaboration
3. Digital content and creation
4. Safety and well-being
5. Problem-solving

And the key activities to develop those skills are:

1. Information gathering
2. Using information creatively
3. Evaluation of information
4. Non-linear thinking
5. Solve problems using IT in creative ways
6. Safety and well-being
7. Collaboration.

We use our Virtual Learning Environment, powered by Microsoft Teams in conjunction with our unique lap top scheme to ensure that every student has access to the curriculum at all times.

Please note that this Policy operates in conjunction with The Use Of Artificial Intelligence Policy 2023.

Digital Safety.

The purpose of this section is to:

- ξ Set out the key principles expected of all members of the school community at Ursuline High School with respect to the use of ICT-based technologies.
- ξ Safeguard and protect the students and staff.
- ξ Assist school staff working with students to work safely and responsibly with the Internet and other IT and communication technologies and to monitor their own standards and practice.
- ξ Set clear expectations of behaviour and/or codes of practice relevant to responsible use of the Internet for educational, personal or recreational use for the whole school community.
- ξ Have clear structures to deal with online abuse such as online bullying which are cross referenced with other school policies.
- ξ Ensure that all members of the school community are aware that unlawful or unsafe behaviour is unacceptable and that, where appropriate, disciplinary or legal action will be taken.
- ξ Minimise the risk of misplaced or malicious allegations made against adults who work with students.

The main areas of risk for our school community can be summarised as follows:

Content

- ⌘ Exposure to inappropriate content, including but not limited to, online pornography, ignoring age ratings in games (exposure to violence associated with often racist language), substance abuse, gambling.
- ⌘ Lifestyle websites, for example pro-anorexia / self-harm / suicide sites
- ⌘ Hate content.
- ⌘ Content validation: how to check authenticity and accuracy of online content.
- ⌘ Students working from home unsupervised and staff working from home for extended periods of time.

Contact

- ⌘ Grooming (sexual exploitation, radicalisation etc.)
- ⌘ Online bullying in all forms.
- ⌘ Social or commercial identity theft (including 'frape' (hacking Facebook profiles)) and sharing passwords.

Conduct

- ⌘ Aggressive behaviours (bullying)
- ⌘ Privacy issues, including disclosure of personal information.
- ⌘ Digital footprint and online reputation.
- ⌘ Health and well-being (amount of time spent online (Internet or gaming)).
- ⌘ Sexting (sending and receiving of personally intimate images) also referred to as SGII (self-generated indecent images) of Youth Produced Sexual Imagery
- ⌘ Copyright (little care or consideration for intellectual property and ownership – such as music and film)

This section applies to all members of Ursuline High School community (including staff, students, volunteers, parents / carers, visitors, community users) who have access to and are users of school systems both in and out of Ursuline High School.

The Education and Inspections Act 2006 empowers Headteachers / Principals to such extent as is reasonable, to regulate the behaviour of students when they are off the school site and empowers members of staff to impose disciplinary penalties for inappropriate behaviour. This is pertinent to incidents of online bullying, or other online safety incidents covered by this policy, which may take place outside of the school, but is linked to membership of the school. The 2011 Education Act increased these powers with regard to the searching for and of electronic devices

and the deletion of data. In the case of both acts, action can only be taken over issues covered by the published Behaviour Policy.

Ursuline High School will deal with such incidents within this policy and associated behaviour and anti-bullying policies and will, where known, inform parents / carers of incidents of inappropriate online safety behaviour that take place out of school.

Key Responsibilities

Headteacher.

Must be adequately trained in off-line and online safeguarding, in-line with statutory guidance.

To lead a 'safeguarding' culture, ensuring that online safety is fully integrated with whole school safeguarding.

To take overall responsibility for online safety provision.

To ensure the school uses appropriate IT systems and services including, filtered Internet Service, e.g. London Grid for Learning (LGfL) services, CPOMS and eForensics.

To be responsible for ensuring that staff receive suitable training to carry out their safeguarding and online safety roles.

To be aware of procedures to be followed in the event of a serious online safety incident.

Ensure suitable 'risk assessments' undertaken so the curriculum meets need of pupils, including risk of children being radicalised.

To receive regular monitoring reports from the Online Safety Co-ordinator during the safeguarding meeting.

To ensure that there is a system in place to monitor and support staff who carry out internal online safety procedures (e.g. network manager).

To ensure Governors are regularly updated on the nature and effectiveness of the school's arrangements for online safety through the pastoral governors forum.

To ensure the school's website includes relevant information.

Online Safety Co-ordinator / Designated Child Safeguarding Officer

Takes day to day responsibility for e-safety issues and has a leading role in establishing and reviewing the school online safety policies / documents.

Promotes an awareness and commitment to online safety throughout the school community.

Ensures that online safety education is embedded across the curriculum.

Liaises with school ICT technical staff where appropriate.

To communicate regularly with SLT and the designated online safety Governor to discuss current issues, review incident logs.

To ensure that all staff are aware of the procedures that need to be followed in the event of an online safety incident.

To ensure that online safety incidents are logged as a safeguarding incident by the safeguarding admin assistant using data from CPOMS and eForensics.

Facilitates training and advice for all staff.

Oversees any student surveys / student feedback on online safety issues.

Liaises with the Local Authority and relevant agencies.

Is regularly updated in online safety issues and legislation and be aware of the potential for serious child protection concerns.

GDPR Officer

Any GDPR breaches or “near Misses” are to be reported to the GDPR officer who will liaise with the relevant agencies, close any loops and take appropriate action. Breaches of GDPR may result in sanctions for staff and the school.

Governors / Safeguarding governor (including online safety)

To ensure that the school has in place policies and practices to keep children and staff safe online.

To approve the Online Safety Policy and review the effectiveness of the policy. This will be carried out by the Governors / Governors Sub Committee receiving regular information about online safety incidents and monitoring reports. A member of the Governing Body has taken on the role of Online Safety Governor.

To support the school in encouraging parents and the wider community to become engaged in online safety activities.

Curriculum Leader

To oversee the delivery of the online safety element of the Computing curriculum.

To liaise with the online safety coordinator regularly.

Id3

To report any online safety related issues that come to their attention, to the Online Safety coordinator.

To manage the school’s computer systems, ensuring:

School password policy is strictly adhered to

Systems are in place for misuse detection and malicious attack (e.g. keeping virus protection up to date).

The school’s policy on web filtering is applied and updated on a regular basis.

That they keep up to date with the school’s online safety policy and technical information in order to effectively carry out their online safety role and to inform and update others as relevant.

That the use of school technology and online platforms are regularly monitored and that any misuse/attempted misuse is reported to the online safety co-ordinator/Headteacher.

To ensure appropriate backup procedures and disaster recovery plans are in place.

To keep up-to-date documentation of the school’s online security and technical procedures.

Teachers

To embed online safety in the curriculum.

To supervise and guide students carefully when engaged in learning activities involving online technology (including, extra-curricular and extended school activities if relevant).

To ensure that students are fully aware of research skills and are fully aware of legal issues relating to electronic content such as copyright laws.

All staff To read, understand, sign and adhere to the school staff Acceptable Use Agreement / Policy, and understand any updates annually. The AUP is signed by new staff on induction.

To be aware of online safety issues related to the use of mobile phones, cameras and handheld devices and that they monitor their use and implement current school policies with regard to these devices.

To ensure that any remote access to School software is only ever done from personal laptops or tablets which are password protected and are solely used by that staff member and not shared with any family member or friend.

To never share their login information and passwords and to report any suspected misuse of their personal devices and access data.

To report any suspected misuse or problem to the online safety coordinator.

To maintain an awareness of current online safety issues and guidance e.g. through CPD.

To model safe, responsible and professional behaviours in their own use of technology.

To ensure that any digital communications with students should be on a professional level and only through school based systems, never through personal mechanisms, e.g. email, text, mobile phones, social media etc.

At the end of the period of employment / volunteering to return and equipment or devices loaned by the school. This will include Usernames and passwords, PINs and to allow devices to be reset or meeting with line manager and technician on the last day to log in and allow a factory reset.

Students

Read, understand, sign and adhere to the Student / Student Acceptable Use Policy.

Have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations.

To understand the importance of reporting abuse, misuse or access to inappropriate materials and never share their login information or passwords.

To know what action to take if they or someone they know feels worried or vulnerable when using online technology.

To know and understand school policy on the use of mobile phones, digital cameras and handheld devices.

To know and understand school policy on the taking / use of images and on online bullying.

To understand the importance of adopting safe behaviours and good online safety practice when using digital technologies out of school and realise that the school's Online Safety Policy covers their actions out of school.

To take responsibility for learning about the benefits and risks of using the Internet and other technologies safely both in school and at home.

To help the school in the creation/ review of online safety policies.

Parents/carers

To monitor their child's use of IT when they are working from home and to ensure that they are logged onto their lessons during any periods of remote learning.

To support the school in promoting online safety and endorse the Parents' Acceptable Use Agreement which includes the students' use of the Internet and the school's use of photographic and video images.

To read, understand and promote the school's Student Acceptable Use Agreement with their children.

To access the school website / on-line student / student records in Progresso in accordance with the relevant school Acceptable Use Agreement.

To consult with the school if they have any concerns about their children's use of technology.

External groups including Parent groups Any external individual / organisation will sign an Acceptable Use Policy prior to using any equipment or the Internet within school.

- To support the school in promoting online safety.
- To model safe, responsible and positive behaviours in their own use of technology.

Student online safety curriculum

This school:

Has a clear, progressive online safety education programme as part of the Computing curriculum / PSHE curriculum. It is built on LA / LGfL online safeguarding and national guidance. This covers a range of skills and behaviours appropriate to their age and experience, including:

- ☞ STOP and THINK before they CLICK.
- ☞ To develop a range of strategies to evaluate and verify information before accepting its accuracy.
- ☞ To be aware that the author of a web site / page may have a particular bias or purpose and to develop skills to recognise what that may be.
- ☞ To know how to narrow down or refine a search; to understand how search engines work and to understand that this affects the results they see at the top of the listings.
- ☞ To understand acceptable behaviour when using an online environment / email, i.e. be polite, no bad or abusive language or other inappropriate behaviour; keeping personal information private.
- ☞ To understand how photographs can be manipulated and how web content can attract the wrong sort of attention.
- ☞ To understand why on-line 'friends' may not be who they say they are and to understand why they should be careful in online environments.
- ☞ To understand why they should not post or share detailed accounts of their personal lives, contact information, daily routines, location, photographs and videos and to know how to ensure they have turned-on privacy settings.
- ☞ To understand why they must not post pictures or videos of others without their permission.
- ☞ To know not to download any files – such as music files - without permission.
- ☞ To have strategies for dealing with receipt of inappropriate materials.
- ☞ To understand why and how some people will 'groom' young people for sexual reasons.
- ☞ To understand the impact of cyberbullying, sexting and trolling and know how to seek help if they are affected by any form of online bullying.
- ☞ To know how to report any abuse including cyberbullying; and how to seek help if they experience problems when using the Internet and related technologies, i.e. parent or carer, teacher or trusted staff member, or an organisation such as ChildLine or the CLICK CEOP button.

Plans Internet use carefully to ensure that it is age-appropriate and supports the learning objectives for specific curriculum areas.

Will remind students about their responsibilities through the Student Acceptable Use Policy which is signed by students and parents in their planner. Students are to be reminded of this by Computing/ICT teachers/tutors/HOY. Ensures staff will model safe and responsible behaviour in their own use of technology during lessons such as ensuring that when using projectors in class all other software (email/Arbor etc.) is closed so there is no possibility of sensitive information being inadvertently shared with students.

Ensures that when copying materials from the web, staff and students understand issues around plagiarism; how to check copyright and also know that they must respect and acknowledge copyright / intellectual property rights.

Ensures that staff and students understand the issues around aspects of the commercial use of the Internet, as age appropriate. This may include, risks in pop-ups; buying on-line; on-line gaming / gambling.

Staff and governor training

This school

Ensures staff know how to send or receive sensitive and personal data and understand the requirement to encrypt data where the sensitivity requires data protection.

Makes regular training available to staff on online safety issues and the school's online safety education program; annual September induction for all staff and regular updates through whole staff training sessions and half termly TED talks.

Provides, as part of the induction process, all new staff [including those on university / college placement and work experience] with information and guidance on the Online Safety policy and the school's Acceptable Use Policies. DSL to undertake relevant training as appropriate.

Parent awareness and training

This school

Provides induction for parents which includes online safety.

Runs a rolling programme of online safety advice, guidance and training for parents

- o This includes induction for parents during tablet distribution
- o Regular update to the online safety information on the school's website and live feeds from external sources within the school website

Handling incidents.

Handling of incidents flow chart for staff during remote learning can be found on the following page.

The school will take all reasonable precautions to ensure online 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. Neither the school nor the Local Authority can accept liability for material accessed, or any consequences of Internet access.

Staff and students are given information about infringements in use and possible sanctions as well as guidance on how to report incidents. Reference in the incident logging template

Online Safety Coordinator acts as first point of contact for any incident.

Any suspected online risk or infringement is reported to the Online Safety Coordinator that day.

Any concern about staff misuse is always referred directly to the Headteacher, unless the concern is about the Headteacher in which case the complaint is referred to the Chair of Governors and the LADO (Local Authority's Designated Officer)

In this school:

There is strict monitoring and application of the online safety policy and a differentiated and appropriate range of sanctions.

Incidents reported from the Smoothwall e-safe system are logged and action taken as appropriate and in line with the schools' policies.

Any child protection issues or contravention of acceptable use are dealt with in accordance with child protection/safeguarding procedures. Evidence is recorded and logged and senior leaders of the school notified immediately.

All members and its wider community are encouraged to be vigilant in reporting issues, in the confidence that issues will be dealt with quickly and sensitively, through the school's escalation processes

Support is actively sought from other agencies as needed (e.g. the Local Authority (LA) and LGFL, UK Safer Internet Centre helpline, CEOP, Prevent Officer, Police and IWF) in dealing with online safety issues

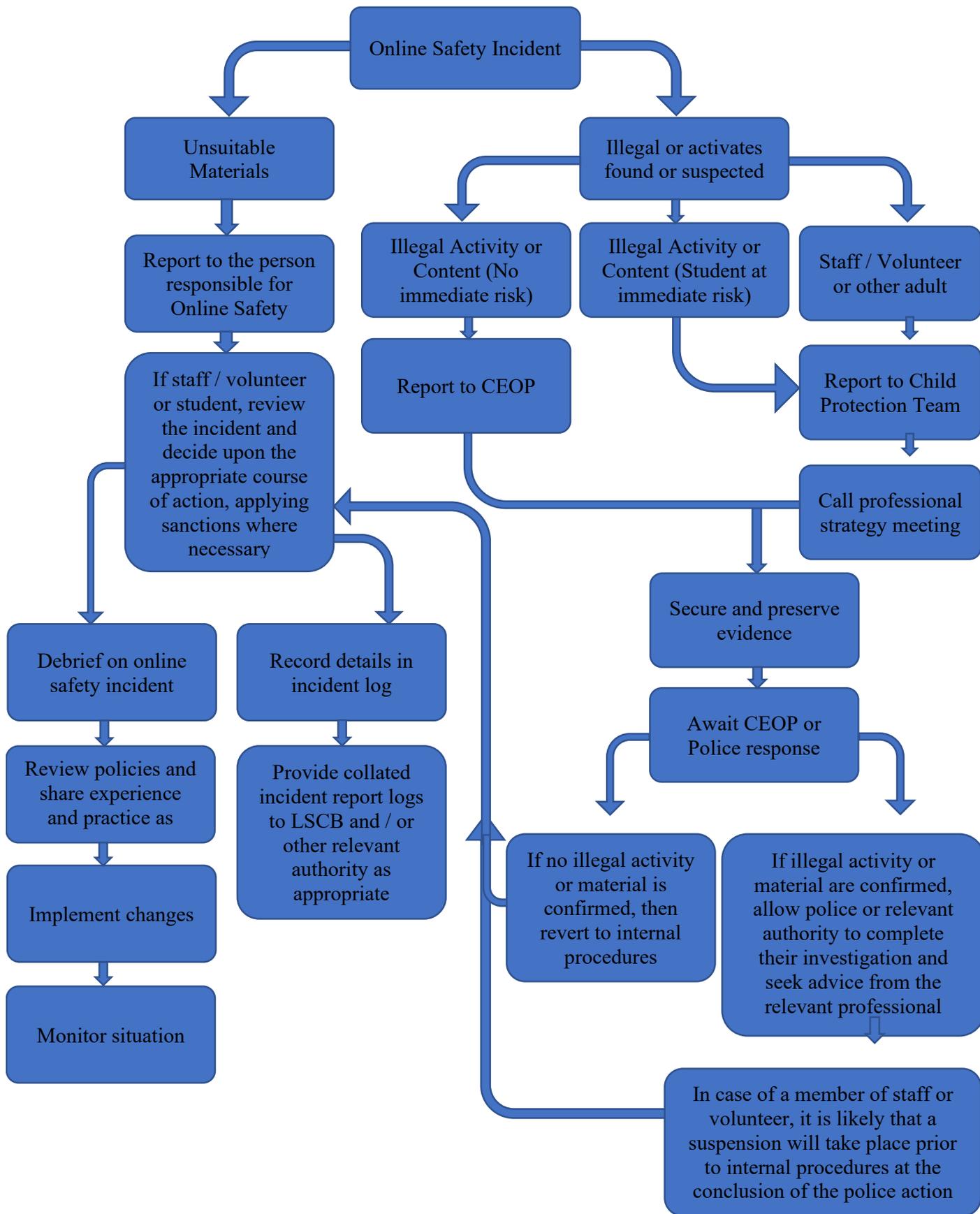
Monitoring and reporting of online safety incidents takes place and contribute to developments in policy and practice in online safety within the school. The records are reviewed / audited and reported to the school's senior leaders including the ICT Strategy Group, Governors / the LA / MSCB

Parents / carers are specifically informed of online safety incidents involving young people for whom they are responsible.

We will contact the Police if one of our staff or students receives online communication that we consider is particularly disturbing or breaks the law.

We will immediately refer any suspected illegal material to the appropriate authorities – Police, Internet Watch Foundation and inform the LA.

Online Safety Incident Flowchart



Remote Learning.

The quality of teaching and learning is at the heart of our policy and should always take precedence over the method or delivery platform.

Research shows that students learn more when they participate in the learning process, whether it's through discussion, practice, review or application. To engage online students, it's important to incorporate activities that allow students to get actively involved.

In the event of school closure, students will continue to follow their regular timetable, with some amendments made to support their wellbeing, as well as our staff, as the need arises. For example, period 1, 3 and 5 will finish ten minutes earlier to give staff and students a screen break.

- In planning their lessons, staff and curriculum leaders are expected to consider the following points
- Feedback. How is this being delivered to students so that they can make progress? What resources are they using to support this?
- How does each department engage with their students? Is their online pedagogy different?
- Are the resources used by the department appropriate and enable students to not only access, but to engage with positively?
- Are HODs, staff and students clear on what students need to learn over the remote learning period and how they will get there? Has the work been planned and sequenced accordingly?
- What is the balance between consolidation and new content? Is it the right balance?
- How are teachers actively involving students?

In the event of school closure, students will continue to follow their regular timetable, with some amendments made to support their wellbeing, as well as our staff, as the need arises. For example, period 1, 3 and 5 will finish ten minutes earlier to give staff and students a screen break.

Staff have undergone rigorous CPD on remote learning and will continue to do so as our pedagogy and ability to deliver outstanding teaching evolves.

Inclusive Learning

We have ensured that every student has access to IT at home. The needs of some students with EHCPs and SEND who are not attending school may also be an issue. Ursuline High School will make use of the TAs and SEND department to support each student and we will endeavour to ensure that all students have access to a tablet and that IT support is continued through ID3.

Wellbeing

The pastoral system at Ursuline High School will continue to provide support for the wellbeing of all students during any remote learning period. This will be done through the Assistant Headteacher Inclusion / Designated Safeguarding Lead via Heads of Year and Tutors. Parents will also be supported in managing their daughter's wellbeing.

Pastoral Care of Pupils

Learning from home can be challenging for a variety of reasons, especially when coupled with social or lifestyle limitations, and possible illness in the family. We appreciate the huge role that parents will be playing and encourage families to structure the day to give balance, variety and a sense of purpose. Parents can play a key role in helping pupils adhere to a routine, and the amount of support will vary depending on the age and personality of the child. Time should be made for regular breaks, exercise, pursuing other

interests (safely within the current social distancing guidelines) and connecting virtually with friends and relatives.

Ursuline High school will also continue to provide a strong sense of pastoral support during the period of closure. Guidance will be offered to parents on supporting their children with remote learning. The school's pastoral support system will also provide a sense of mental and emotional wellness, in addition to ensuring our most vulnerable students will continue to receive focused pastoral support.

Monitoring, review & evaluation

Ursuline High School is committed to ensuring that Remote Teaching and Learning is evaluated and monitored to ensure that it is of the highest quality.

Monitoring can be carried out through the follow means:

- Physical learning walks from Middle and Senior Leaders if staff are teaching on site.
- Virtual Learning walks using URL for each team. Conducted by Middle and Senior Leaders.
- Current policy states that there should be 3 learning walks per HOD/HOF/KsC per half term (not including revisits or follow up observations). There needs to be at least one Virtual and one Physical learning walk in each half term. The third needs to be based on identified gaps and needs. A learning walk is one lesson where you will observe 2 to 3 different teachers using the Learning walk proforma.
- Book scrutiny – the first of the academic year is the equivalent of checking all books have tracking sheets, pedagogy and big picture on covers etc. The next 2 will be a more formal book scrutiny with a proforma for feedback.
- To monitor books, the subject teacher can click on the “Manage Notebook” icon and share the link for the class.
- Assignments – feedback given through assignments should be added to the Grade Tracking sheet. This can be checked by middle leaders during book scrutiny. The teacher can also send all the marking and feedback from the work by clicking on “Export to Excel” icon.

The following assessment measures are also used regularly by SLT, HOF, HOD and Key stage coordinators:

- Students surveys.
- Staff surveys.
- CPD evaluations from staff.
- Departmental, Heads of Faculty, SLT meetings.
- Weekly Quality of Education meeting involving senior leaders.
- Weekly IT meeting with Headteacher, ID3 and Digital Learning coordinator.
- T&L feedback proforma from Heads of Department.

The School Development Plan will be amended based on monitoring and feedback.

Guidelines for staff when using remote learning through MS Teams at home.

Before a member of staff can use microphones or the video function in their teaching, they need to read this document and then email Assistant Head Teacher Teaching and Learning / Digital Learning (Owen Nichols) to confirm that they have read and understood this document.

Please note that staff can use Microphones only and not the Camera option if they prefer.

General Guidelines

- i. The Video Function is to be blurred or other background used. This can only be done on the App, not when accessing Teams through the VLE link on the website. Click on the 3 dots during a meeting.
- ii. Staff are to be dressed appropriately as they would when teaching in the classroom. This includes having your lanyard on.
- iii. Staff are to conduct themselves in the same professional manner expected when in the classroom.
- iv. The mic and video function is to be switched off when not needed. Staff are to have clear planning on when to use it and justify that decision. The video and mic are to be used for specific tasks.
- v. To be conducted in a quiet area in your home. Only the teacher is to be heard, so take background noise and household members into consideration.
- vi. Students can still type in questions for staff to answer verbally.
- vii. When sharing your desktop in your teaching, make sure that all emails and sensitive documents are closed to avoid any GDPR breaches.

Student microphones

- i. Students are to only have microphone on when directed by teacher and then switched off afterwards.
- ii. Students should only have microphone on when working in a quiet area with no distracting noise.
- iii. Students are to speak and behave as they would according to the school behaviour policy. Students are to be reminded as such at the beginning of the session.
- iv. Non compliance will result in the teacher muting the students' microphone.

Safeguarding

- i. All lessons using microphone or cameras are to be recorded. Click on the 3 dots and then start recording. This will be saved in the Posts channel for the Team. Only those who are part of the Team will be able to view this recording. These can be viewed by SLT for safeguarding purposes.
- ii. Staff should mute a student if necessary and know how to do this before any meeting starts.
- iii. From September 2020, all students will have the video function on and dressed in school uniform.

STAFF ARE TO FOLLOW SCHOOL SAFEGUARDING POLICY AT ALL TIMES. THIS INCLUDES THE USE OF CPOMS.

Managing online learning: Roles & Responsibilities

The Governors agree the Remote Teaching and Learning Policy and monitor its implementation through the Curriculum Committee. The governing body receives an annual report from the Senior Leader on its implementation.

Senior Leadership Team: Assistant Head Teacher

- Ensures that Teaching and Learning meets the needs of all learners in KS3, 4&5.
- Feeds into the SDP.
- Monitors and reviews the implementation of Teaching and Learning.
- Supports the Strategic Quality of Education group.
- Provides clear expectations of Teaching and Learning.
- Receives and investigates parental complaints relating to remote Teaching and Learning.
- Maintains an informed overview about the quality of teaching across each key stage and the outcome priorities needed for individual students.
- Consults on agreed organisational matters relating to remote teaching and learning.
- Ensures that statutory curriculum requirements are met.
- Ensures that staff and students are appropriately trained in the use of Remote Learning tools.
- Liaises with HODs and Digital Learning Coordinator on the use of subject specific Apps and Learning tools.

Quality of education Strategy Group

- Acts as a steering group for the half termly Key Stage Teaching & Learning meetings.
- Provides strategic direction in terms of pedagogy, research and best teaching practices.

Heads of Faculty & Department

- Ensure that the curriculum meets the needs of all learners in their subject/s.
- Provide strategic overview for their subjects/s, linked to the School Improvement Plan.
- Review and consult on choice of syllabus at GCSE & Post 16 for their subject.
- Manage, coach & lead their key stage co-ordinators as appropriate.
- Keep abreast of developments in their subject/s, updating SLT as needed, by attending relevant CPD and ensuring that all staff within the Faculty undergo relevant CPD as required.
- Ensure that Schemes of Learning are reviewed, quality assured and delivered appropriately by teaching staff.
- Monitor the standard & quality of teaching & learning in their areas.
- Develop & review annually a cohesive curriculum plan for their subject/s that is challenging, inspiring and accessible to all students.
- Ensure that students' intervention entitlements continue to be met

Heads of Year

- Ensures that the curriculum meets the needs of all learners in their year group.
- Evaluate the impact of strategies used to support teaching and learning through Year Team reviews.
- Monitor the impact of the curriculum on the progress of individuals & specific groups through report cards, interviews, work samples etc.
- Liaise with HODS/HOFS as necessary in supporting individual students & specific groups.
- Monitor the setting of homework for their year group through book & planner sampling.
- Work with AHTs to ensure that students make informed choices about options, courses & Pathways.
- Liaise with parents/guardians where students need support across subjects.
- Ensure that external providers meet the needs of our students.

Tutors

- Monitor the progress of students in their tutor group.
- Work with HOY to ensure that students make informed choices about options, courses & pathways.
- Liaises with parents/guardians where students need support across subjects.

Managing the ICT infrastructure

Internet access, security (virus protection) and filtering

This school

- ξ Accepts that Filtering and monitoring systems are only ever tools in helping to safeguard children when online and this school has an obligation to “consider how children may be taught about safeguarding, including online, through teaching and learning opportunities, as part of providing a broad and balanced curriculum.”
- ξ Informs all users that all IT use including internet / email use is monitored.
- ξ Has the educational filtered secure broadband connectivity through the LGfL (Regional Broadband Consortium).
- ξ Uses Smoothwall e-safe to monitor all IT use on all school owned devices, monitoring onsite and offsite activity.
- ξ Uses the LGfL Web Screen filtering system which blocks sites that fall into categories such as pornography, race hatred, gaming, sites of an illegal nature, etc. The filtering system is appropriate and in line with DfE and UK Safer Internet Centre guidance. All changes to the filtering policy are logged and only available to staff with the approved ‘web filtering management’ status.
- ξ Uses USO user-level filtering where relevant, thereby closing down or opening up options appropriate to staff and the age appropriate expectations of pupils.
- ξ Ensures network health through use of Sophos anti-virus software (from LGfL) etc.
- ξ Uses DfE, LA or LGfL approved systems such as S2S, LGFL USO FX2, secured email to send ‘protect-level’ (sensitive personal) data over the Internet.
- ξ Blocks all Chat rooms and social networking sites except those that are part of an educational network or approved Learning Platform.
- ξ Only unblocks other external social networking sites for specific purposes / Internet Literacy lessons.
- ξ Has blocked student access to music download or shopping sites – except those approved for educational purposes at a regional or national level, such as Audio Network.
- ξ Uses security time-outs on Internet access where practicable / useful.
- ξ Works in partnership with the LGfL to ensure any concerns about the system are communicated so that systems remain robust and protects students.
- ξ Is vigilant in its supervision of students’ use at all times, as far as is reasonable, and uses common-sense strategies in learning resource areas where older students have more flexible access.
- ξ Ensures all staff and students have signed an acceptable use agreement form and understands that they must report any concerns.
- ξ Ensures students only publish within an appropriately secure environment: the school’s learning platform and school approved platforms.
- ξ Requires staff to preview websites before use [where not previously viewed or cached] and encourages use of the school’s Learning Platform as a key way to direct students to age / subject appropriate web sites is vigilant when conducting ‘raw’ image search with students e.g. Bing image search.
- ξ Informs staff and students that that they must report any failure of the filtering systems directly to the Network Manager. Our Network Manager logs or escalates as appropriate to the Technical service provider or LGfL Helpdesk as necessary.
- ξ Makes clear all users know and understand what the ‘rules of appropriate use’ are and what sanctions result from misuse – through staff meetings and teaching programme.
- ξ Provides advice and information on reporting offensive materials, abuse/ bullying etc. available for students, staff and parents.
- ξ Immediately refers any material we suspect is illegal to the appropriate authorities – Police – and the LA.

Network management (user access, backup)

This school

- ⌘ Uses individual, audited log-ins for all users.
- ⌘ Uses guest accounts occasionally for external or short term visitors for temporary access to appropriate services.
- ⌘ Uses teacher 'remote' monitoring tools for viewing users applications and Internet web sites, where appropriate.
- ⌘ Has additional local network auditing software installed (System Centre Configuration Manager).
- ⌘ Ensures the Network Manager is up-to-date with LGfL services and policies / requires the Technical Support Provider to be up-to-date with LGfL services and policies.
- ⌘ Has daily backup of school data
- ⌘ Uses secure, Microsoft Azure cloud storage for remote data backup. Online backups are always encrypted.
- ⌘ Storage of all data within the school will conform to the GDPR requirements

To ensure the network is used safely, this school:

- ⌘ Ensures staff read and sign that they have understood the school's Online Safety Policy. Following this, they are set-up with Internet, email access and network access. Online access to service is through a unique, audited username and password. We also use the same username and password for access to our school's network where necessary.
- ⌘ Staff access to the schools' management information system is controlled through a separate means of authentication for data security purposes.
- ⌘ We provide students with an individual network log-in username. From Year 7 they are also expected to use a personal password.
- ⌘ All students have their own unique username and password which gives them access to the Internet, the Learning Platform and their own school approved email account.
- ⌘ Access to the School's network and software is removed for all leavers in accordance with GDPR requirements.
- ⌘ Makes clear that no one should log on as another user and makes clear that students should never be allowed to log-on or use teacher and staff logins.
- ⌘ Has set-up the network with a shared work area for students and one for staff. Staff and students are shown how to save work and access work from these areas.
- ⌘ Requires all users to always log off when they have finished working or are leaving the computer unattended.
- ⌘ Where a user finds a logged-on machine, we require them to always log-off and then log-on again as themselves.
- ⌘ Requests that teachers and students do not switch the computers off during the day unless they are unlikely to be used again that day or have completely crashed.
- ⌘ Acknowledges that data protection is key in schools and, as more teachers have access to high level pupil information through access to Schools MIS systems and requires staff to ensure their computer is locked or logged off when not in use.
- ⌘ Ensures all equipment owned by the school or connected to the network has up to date virus protection.
- ⌘ Makes clear that staff are responsible for ensuring that any device loaned to them by the school, is used solely to support their professional responsibilities and that they notify the school of any "significant personal use" as defined by HM Revenue & Customs.
- ⌘ Makes clear that staff accessing LA systems do so in accordance with any Corporate policies.
- ⌘ Makes clear that staff must not access any system remotely or online which contains or allows the download of any staff related records, with the exception of Arbor (which does not contain sensitive staff records), on any device which is not owned by the school. This includes HR, Payroll and spreadsheets which contain staff

records. Student and parent information which is highly confidential e.g. Health Records and Vulnerable child records are also classified as highly sensitive.

- ⌘ Maintains equipment to ensure Health and Safety is followed.
- ⌘ Keeps an asset log of all equipment including equipment allocated to individuals.
- ⌘ Has integrated curriculum and administration networks, but access to the staff Management Information System is set-up so as to ensure staff users can only access modules related to their role.
- ⌘ Does not allow any outside Agencies to access our network remotely except where there is a clear professional need and then access is audited and restricted and is only through approved systems.
- ⌘ Has a clear disaster recovery system in place for critical data that includes a secure, remote offsite back up of data.
- ⌘ Uses secure data transfer, the DfE secure s2s website for all CTF files sent to other schools and the LA.
- ⌘ Ensures that all student level data or personal data sent over the Internet is encrypted or only sent within the approved secure system in our LA or through USO secure file exchange (USO FX2) – nominated staff only.
- ⌘ Follows ISP advice on Local Area and Wide Area security matters and firewalls and routers have been configured to prevent unauthorised use of our network.
- ⌘ Our wireless network has been secured to industry standard Enterprise security level /appropriate standards suitable for educational use;
- ⌘ All IT and communications systems are installed professionally and regularly reviewed to ensure they meet health and safety standards.
- ⌘ Projectors are maintained so that the quality of presentation remains high.
- ⌘ Reviews the school ICT systems regularly with regard to health and safety and security.

Password policy

This school makes it clear that staff and students must always keep their password private, must not share it with others. They must also not allow another user to use their own account on any devices or system. They will notify the school if they suspect their account has been compromised.

Username and passwords are unique to each pupil at an appropriate level of complexity for the age range.

All staff have their own unique username and private passwords to access school systems. Staff are responsible for keeping their password(s) private.

We require staff to use STRONG passwords. Strong Passwords are at least seven characters and have a combination of upper and lower case letters, numbers and the special keyboard characters like the asterisk or currency symbols.

<https://www.cyberaware.gov.uk/passwords>

We require staff to change their passwords into the MIS, LGfL USO admin site at least twice a year.

E-mail

This school

Provides staff with an email account for their professional use and makes clear personal email should be through a separate account.

Does not publish personal e-mail addresses of students or staff on the school website. We do not publish student emails, but we do publish staff school email address. Class email addresses can only receive emails from staff email addresses.

Will contact the Police if one of our staff or students receives an e-mail that we consider is particularly disturbing or breaks the law.

Will ensure that email accounts are maintained and up to date.

Reports messages relating to or in support of illegal activities to the relevant Authority and if necessary to the Police.

Knows that spam, phishing and virus attachments can make emails dangerous. We use a number of LGfL-provided technologies to help protect users and systems in the school, including desktop anti-virus product Sophos, plus direct email filtering for viruses, Trojans, pornography, phishing and inappropriate language. LGfL WebScreen2 filtering monitors and protects our Internet access to the World Wide Web.

Students

Students should only receive external mail from and send external mail to acceptable addresses.

Students are taught about the safety and 'netiquette' of using e-mail both in school and at home i.e. they are taught:

- ☞ Not to give out their e-mail address unless it is part of a school managed project or to someone they know and trust and is approved by their teacher or parent/carer.
- ☞ That an e-mail is a form of publishing where the message should be clear, short and concise.
- ☞ That any e-mail sent to an external organisation should be written carefully and authorised before sending, in the same way as a letter written on school headed paper.
- ☞ They must not reveal private details of themselves or others in e mail, such as address, telephone number, etc.
- ☞ To 'Stop and Think Before They Click' and not open attachments unless sure the source is safe.
- ☞ That they should think carefully before sending any attachments.
- ☞ Embedding adverts is not allowed.
- ☞ That they must immediately tell a teacher / responsible adult if they receive an e-mail which makes them feel uncomfortable, is offensive or bullying in nature.
- ☞ Not to respond to malicious or threatening messages.
- ☞ Not to delete malicious or threatening e-mails, but to keep them as evidence of bullying.
- ☞ Not to arrange to meet anyone they meet through e-mail without having discussed with an adult and taking a responsible adult with them.
- ☞ That forwarding 'chain' e-mail letters is not permitted.

Students sign the school Agreement Form to say they have read and understood the online safety rules, including e-mail and we explain how any inappropriate use will be dealt with.

Staff

Access in school to external personal e mail accounts may be blocked.

Staff will use the school email systems for professional purposes only.

Staff will ensure that any remote access to School software is only ever done from School owned devices, which are password protected and had 2 factor authentication.

No USB storage devices are to be used for any reason.

Staff will never share their login information and passwords and will report any suspected misuse of their personal devices and access data.

Never use email to transfer staff or student personal data. 'Protect-Level' data should never be transferred by email. Staff must use secure, LA / DfE approved systems to transfer 'Protect-Level' data. These include: S2S (for school to school transfer); Collect; USO-FX2

Staff know that e-mail sent to an external organisation must be written carefully, (and may require authorisation), in the same way as a letter written on school headed paper. That it should follow the school policy.

All staff sign our school Agreement Form AUP to say they have read and understood the e-safety rules, including e-mail and we explain how any inappropriate use will be dealt with.

School website

The Headteacher takes overall responsibility to ensure that the website content is accurate and the quality of presentation is maintained

Uploading of information is restricted to our website authorisers: Marketing and Communications Officer

The school web site complies with the statutory DfE guidelines for publications.

Most material is the school's own work; where other's work is published or linked to, we credit the sources used and state clearly the author's identity or status.

Photographs published on the web do not have full names attached.

We do not use students' names when saving images in the file names or in the tags when publishing to the school website.

We do not use embedded geodata in respect of stored images.

We expect teachers using' school approved blogs or wikis to password protect them.

Learning platform

Our school learning platform utilises Microsoft Teams.

Uploading of information on the schools' online learning space is shared between different staff members according to their responsibilities e.g. all class teachers upload information in their class areas.

Photographs and videos uploaded to the school's online environment will only be accessible by members of the school community.

In school, students are only able to upload and publish within school approved and closed systems, such as the Learning Platform.

Social networking

Staff are instructed to always keep professional and private communication separate.

Teachers are instructed not to run social network spaces for student use on a personal basis or to open up their own spaces to their students, but to use the schools' preferred system for such communications.

The school's preferred system for social networking (externally, only through approved Twitter accounts) will be maintained in adherence with the communications policy.

School staff will ensure that in private use:

No reference should be made in social media to students, parents / carers or school staff.

School staff should not be online friends with any student. Any exception must be approved by the Headteacher.

They do not engage in online discussion on personal matters relating to members of the school community.

Personal opinions should not be attributed to the school or local authority and personal opinions must not compromise the professional role of the staff member, nor bring the school into disrepute.

Security settings on personal social media profiles are regularly checked to minimise risk of loss of personal information.

Students.

Are taught about social networking, acceptable behaviours and how to report misuse, intimidation or abuse through our online safety curriculum work.

Students are required to sign and follow our student acceptable use agreement

Parents.

Parents are reminded about social networking risks and protocols through our parental acceptable use agreement and additional communications materials when required.

Are reminded that they need to ask permission before uploading photographs, video or any other information about other people.

CCTV

We have CCTV in the school as part of our site surveillance for staff and student safety. The use of CCTV is clearly signposted in the school. We will not reveal any recordings without permission except where disclosed to the Police as part of an investigation.

We use specialist lesson recording equipment on occasions as a tool to share best teaching practice. We do not reveal any such recordings outside of the staff and will not use for any other purposes.

Equipment and Digital Content

Currently the school WiFi setup for all users is on the same network.

Personal mobile phones and mobile devices

Mobile phones brought into school are entirely at the staff member, student's and parents' or visitors own risk. The School accepts no responsibility for the loss, theft or damage of any phone or hand held device brought into school.

The school has provided a mobile phone for the HeadTeacher and the DSL. During school visits, school mobiles are provided for trip leaders. During periods of remote learning, Heads of Year, PSAs, Student Services (Including 6th form), HLTAs, SENCO and identified members of the safeguarding team will be provided with a school mobile phone.

Student mobile phones which are brought into school must be turned off (not placed on silent) and stored out of sight on arrival at school. They must remain turned off and out of sight until the end of the day. Staff members may use their phones during school break times and away from students.

The recording, taking and sharing of images, video and audio on any mobile phone is not permitted; except where it has been explicitly agreed otherwise by the Headteacher. Such authorised use is to be monitored and recorded. All mobile phone use is to be open to scrutiny and the Headteacher is to be able to withdraw or restrict authorisation for use at any time if it is to be deemed necessary.

In line with current legislation (The Education Act 2011) the School reserves the right to search the content of any mobile or handheld devices on the school premises where there is a reasonable suspicion that it may contain undesirable material, including those which promote pornography, violence or bullying. Staff mobiles or hand held devices may be searched at any time as part of routine monitoring.

Where parents or students need to contact each other during the school day, they should do so only through the School's telephone system. Staff may use their phones during break times. If a staff member is expecting a personal call they may leave their phone with the school office to answer on their behalf, or seek specific permissions to use their phone at other than their break times.

Mobile phones and personally-owned devices will not be used in any way during lessons or formal school time. They should be switched off or silent at all times.

Mobile phones and personally-owned mobile devices brought in to school are the responsibility of the device owner. The school accepts no responsibility for the loss, theft or damage of personally-owned mobile phones or mobile devices.

Mobile phones will not be used during lessons or formal school time unless as part of an approved and directed curriculum-based activity with consent from a member of staff.

The Bluetooth or similar function of a mobile phone should be switched off at all times and not be used to send images or files to other mobile phones.

No images or videos should be taken on mobile phones or personally-owned mobile devices without the prior consent of the person or people concerned.

Students' use of personal devices

The School strongly advises that student mobile phones should not be brought into school.

The School accepts that there may be particular circumstances in which a parent wishes their child to have a mobile phone for their own safety.

If a student breaches the school policy, then the phone or device will be confiscated and will be held in a secure place in the student services office. Mobile phones and devices will be released to parents or carers in accordance with the school policy.

Phones and devices must not be taken into examinations. Students found in possession of a mobile phone during an exam will be reported to the appropriate examining body. This may result in the student's withdrawal from either that examination or all examinations.

If a student needs to contact his or her parents or carers, they will be allowed to use a school phone. Parents are advised not to contact their child via their mobile phone during the school day, but to contact the school office.

Students should protect their phone numbers by only giving them to trusted friends and family members. Students will be instructed in safe and appropriate use of mobile phones and personally-owned devices and will be made aware of boundaries and consequences.

Staff use of personal devices

Staff are not permitted to use their own mobile phones or devices for contacting children, young people or their families within or outside of the setting in a professional capacity, unless agreed with the Headteacher.

Staff will be issued with a school phone where contact with students, parents or carers is required.

Mobile Phones and personally-owned devices will be switched off or switched to 'silent' mode. Bluetooth communication should be 'hidden' or switched off and mobile phones or personally-owned devices will not be used during teaching periods unless permission has been granted by a member of the senior leadership team in emergency circumstances.

If members of staff have an educational reason to allow children to use mobile phones or a personally-owned device as part of an educational activity, then it will only take place when approved by the senior leadership team.

Staff should not use personally-owned devices, such as mobile phones or cameras, to take photos or videos of students and will only use - school owned equipment for this purpose.

If a member of staff breaches the school policy, then disciplinary action may be taken.

Where staff members are required to use a mobile phone for school duties, for instance in case of emergency during off-site activities, or for contacting students or parents, then a school mobile phone will be provided and used. In an emergency where a staff member doesn't have access to a school-owned device, they should use their own device and hide (by inputting 141) their own mobile number for confidentiality purposes.

Digital images and video

In this school:

We gain parental / carer permission for use of digital photographs or video involving their child as part of the school agreement form when their daughter joins the school.

We do not identify students in online photographic materials or include the full names of students in the credits of any published school produced video materials.

Staff sign the school's Acceptable Use Policy and this includes a clause on the use of mobile phones / personal equipment for taking pictures of students.

Images should not be left on school owned devices or memory cards. Images should be stored on the school central areas and securely deleted if no longer required.

If specific student photos (not group photos) are used on the school web site, in the prospectus or in other high profile publications the school will obtain individual parental or student permission for its long term use.

The school blocks/filter access to social networking sites or newsgroups unless there is a specific approved educational purpose.

Students are taught about how images can be manipulated in their online safety education programme and also taught to consider how to publish for a wide range of audiences which might include governors, parents or younger children as part of their ICT scheme of work.

Students are advised to be very careful about placing any personal photos on any 'social' online network space. They are taught to understand the need to maintain privacy settings so as not to make public, personal information.

Students are taught that they should not post images or videos of others without their permission. We teach them about the risks associated with providing information with images (including the name of the file), that reveals the identity of others and their location, such as house number, street name or school. We teach them about the need to keep their data private and what to do if they are subject to bullying or abuse.

Appendices.

Acceptable Use Policies and Agreement

Ursuline High School regularly reviews and updates all Acceptable Use documents to ensure that they are consistent with the school Online Safety and Safeguarding Policies. We attempt to ensure that all students have good access to digital technologies to support their teaching and learning and we expect all our students to agree to be responsible users to help keep everyone safe and to be fair to others.

Parents Acceptable Use Agreement

Internet and IT: As the parent or legal guardian of the student(s) named below, I grant permission for the school to give my daughter access to:

the Internet at school

the school's chosen email system

the school's online virtual learning environment 'MS Teams'

IT facilities, equipment and software at the school

Devices given to student to extend their use of IT outside of school

I understand that the school uses monitoring software to monitor the use of all school owned devices and that this monitoring software is active even when the device is outside of school and in my home.

I accept that ultimately the school cannot be held responsible for the nature and content of materials accessed through the Internet and mobile technologies, but I understand that the school takes every reasonable precaution to keep pupils safe and to prevent students from accessing inappropriate materials.

I agree that while my daughter is using IT at home, I will take reasonable precautions to keep my daughter safe and promote safe and responsible use of IT. I will support and monitor my daughter in any online learning.

Use of digital images, photography and video:

I understand the school has a clear policy on "The use of digital images and video" and I support this.

I understand that the school will necessarily use photographs of my daughter or including them in video material to support learning activities.

I accept that the school may use photographs / video that includes my daughter in publicity that reasonably promotes the work of the school, and for no other purpose.

Social networking and media sites:

I understand that the school has a clear policy on "The use of social networking and media sites" and I support this. I will not take and then share online, photographs, videos etc., about other student (or staff) at school events, without permission. I understand that the school takes any inappropriate behaviour seriously and will respond to observed or reported inappropriate or unsafe behaviour. I will support the school by promoting safe and responsible use of the Internet, online services and digital technology at home. I will inform the school if I have any concerns.

Student name: _____

Parent / guardian signature: _____

Date: ___/___/___

The use of digital images and video

To comply with GDPR, we need your permission before we can photograph or make recordings of your daughter.

Ursuline High School rules for any external use of digital images are:

If the student is named, we avoid using their photograph.

If their photograph is used, we avoid naming the student.

Where showcasing examples of students work or achievements we only use their first name, rather than their full names.

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

Only images of students 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 at school include:

Your daughter being photographed (by the class teacher or teaching assistant) as part of a learning activity;

e.g. taking photos or a video of progress made of students in music or drama, as part of the learning record, and then sharing with their parent / guardian.

Your daughter's image being used for presentation purposes around the school;

e.g. in class or wider school wall displays or PowerPoint© presentations.

Your daughter'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 daughter's picture could appear in the media if a newspaper photographer or television film crew attends an event.

Note: If we, or you, actually wanted your daughter's image linked to their name we would contact you separately for permission.

e.g. if your daughter won a national competition and wanted to be named in local or government literature.

The use of social networking and online media

This school asks its whole community to promote the 3 commons approach to online behaviour:

Common courtesy

Common decency

Common sense

How do we show common courtesy online?

We ask someone's permission before uploading photographs, videos or any other information about them online.

We do not write or upload 'off-hand', hurtful, rude or derogatory comments and materials. To do so is disrespectful and may upset, distress, bully or harass.

How do we show common decency online?

We do not post comments that can be considered as being intimidating, racist, sexist, homophobic or defamatory. This is online-bullying and may be harassment or libel.

When such comments exist online, we do not forward such emails, tweets, videos, etc. By creating or forwarding such materials we are all liable under the law.

How do we show common sense online?

We think before we click.

We think before we upload comments, photographs and videos.

We think before we download or forward any materials.

We think carefully about what information we share with others online, and we check where it is saved and check our privacy settings.

We make sure we understand changes in use of any web sites we use.

We block harassing communications and report any abuse.

Any actions online that impact on the school and can potentially lower the school's (or someone in the school) reputation in some way or are deemed as being inappropriate will be responded to.

In the event that any member of staff, student or parent/carer is found to be posting libellous or inflammatory comments on Facebook or other social network sites, they will be reported to the appropriate 'report abuse' section of the network site and/or police where appropriate.

(All social network sites have clear rules about the content which can be posted on the site and they provide robust mechanisms to report contact or activity which breaches this.)

In serious cases we will also consider legal options to deal with any such misuse.

Student Acceptable Use Policy

Online Safety Agreement & Acceptable Use of ICT & Social Media

Ursuline High School has a curriculum computer network which full internet access to assist learning. Students can use this facility only when parents/guardians have signed this agreement.

Digital Wisdom:

If you receive abusive messages, keep them. You do not have to read them. When the time comes for action they can be used as evidence. If you receive abusive message ask for help from parents/carer, your Form Tutor, Head of Year, School Nurse or School Counsellor. You can also contact your mobile phone provider. Remember: by forwarding a text, email, photo, video, etc, you may be making the problem worse. You could be unwittingly involving yourself in bullying. You may even be breaking the law.

I agree to:

1. I will keep my login and password details secret and will not access anyone else's files.
2. I will only use the computers for schoolwork and homework.
3. I will not bring files into school that can harm the school network or be used to compromise school security tools.
4. I will only use the internet for appropriate educational purposes.
5. I will not use messaging software or clients.
6. I will use polite standard English in all communications and good email etiquette at all times. Such as: Dear, Thank you, Please, etc.
7. I will not give my personal information that could be used to identify me, my family or friends on any space, unless a trusted adult has given me permission or reviewed the site.
8. I understand that my files will be checked and that my use of the internet will be monitored.
9. I understand that the use of all school devices is monitored inside and outside of the school including use at home. Any activity which is considered to contravene this agreement or may be considered to fall within the schools safeguarding requirements is automatically reported to the school.
10. I will not undertake any activity. including loading software, that is found to threaten the integrity of the computer network or attacks or corrupts other systems.
11. I will respect the copyright of materials.
12. I will not use any digital device to access, post or produce anonymous messages; material of an inappropriate, threatening, discriminatory, racist, homophobic or offensive nature. I will not post derogatory or negative comments about the school or any member of the school community.
13. I will not post/upload on the internet or social network any materials which can cause damage to my personal reputation, other people's reputation or the reputation of the school.
14. I will not post or upload any materials or photos which can identify the school and breach the safety of students on any social networks such as Youtube/Facebook/msn/Ask FM/Twitter/Snapchat/Instagram/WhatsApp/. I will respect the required age to create accounts on social networks.
15. I will follow all the guidance provided by school on the safe use of my laptop/tablet and take care of my school laptop/tablet and protect it from damage. I understand that insurance cover is limited.
16. I will respect the school computer hardware and not abuse it.
17. I will report to a member of staff, any videos or materials, showing the school buildings or students in uniform, posted on the web without the school's permission.
18. Breaching any of the above will be subject to an appropriate sanction, which may result in withdrawal of Internet access in school and ultimately in an exclusion.
19. In line with the Social Media Policy, we reserve the right to look at the students' mobile phones and laptops when conducting investigations

20. I will never arrange to meet someone I have only ever previously met on the internet, by email or in a chat room, unless it take a trusted adult.

21. If I see anything I am unhappy with or receive a message that makes me feel uncomfortable, I will not respond to it but I will save it and talk to a trusted adult.

Student's Signature Date

As the parent/carer of the student signing above, I grant permission for my daughter to use email and the internet. I understand that students will be held accountable for their actions. I also understand that some materials on the internet may be objectionable and I accept joint responsibility for the setting of standards for my daughter to follow when selecting, sharing and exploring information and media. I will also check her mobile devices on a regular basis to ensure her safety and will make sure appropriate filters are in place at home.

Parent/Carer's Signature Date

Acceptable Use Agreement: All Staff, Volunteers, Contractors and Governors

Covers use of all digital technologies in school: i.e. email, Internet, intranet, network resources, learning platform, software, communication tools, social networking tools, school website, equipment and systems.

Ursuline High School regularly reviews and updates all AUA documents to ensure that they are consistent with the school Online Safety Policy.

These rules will help to keep everyone safe and to be fair to others. School systems and users are protected and monitored by security and filtering services to provide safe access to digital technologies.

I will only use the school's digital technology resources and systems for Professional purposes or for uses deemed 'reasonable' by the Head and Governing Body.

I will not reveal my password(s) to anyone or let any other individual knowingly use my account(s).

When working remotely, I will only access the School's software (ie email or Progresso) from a personal laptop or tablet which is password protected and is solely used by me and not shared with any family member or friend.

I will never access the School's software from a public device

I will follow school procedures in the creation and use of my password (must not contain any part of your username or full name, must contain characters from 3 of the following 4: upper case (A-Z), lower case (A-Z), numbers (0-9), symbols e.g. £,!,*). If my password is compromised, I will ensure I change it. I will not use anyone else's password if they reveal it to me and will advise them to change it.

I will not allow unauthorised individuals to access email / Internet / intranet / network, or other school systems, or any system I have access to.

I will ensure all documents, data etc., are printed, saved, accessed and deleted / shredded in accordance with the school's network and data security protocols.

I will not engage in any online activity that may compromise my professional responsibilities.

I will only use the approved email system(s) for any school business.

I will only use the approved email system (UHSW email / Webmail), Learning Platform (Frog) and school approved communication systems with pupils or parents/carers, and only communicate with them on appropriate school business.

I will not support or promote extremist organisations, messages or individuals.

I will not give a voice or opportunity to extremist visitors with extremist views.

I will not browse, download or send material that is considered offensive or of an extremist nature by the school.

I will report any accidental access to, or receipt of inappropriate materials, or filtering breach or equipment failure to the appropriate line manager, ICO and / or Online Safety Co-ordinator.

I will not download any software or resources from the Internet that can compromise the network or might allow me to bypass the filtering and security system or are not adequately licensed.

I will check copyright and not publish or distribute any work including images, music and videos, that is protected by copyright without seeking the author's permission.

Any data and material brought onto the school site and / or onto the school network must be appropriate for the school environment. The Headteacher and / or authorised staff have the right to view all data without consent.

I will not connect any device (including USB flash drive), to the network that does not have up-to-date anti-virus software, and I will keep any 'loaned' equipment up-to-date, using the school's anti-virus and other Smoothwall e-safe systems.

I will not use personal digital cameras or camera phones or digital devices for taking, editing and transferring images or videos of pupils or staff and will not store any such images or videos at home or on any personal devices.

I will follow the school's policy on use of mobile phones / devices at school and will not take into classrooms / only use in staff areas.

I will only use school approved equipment for any storage, editing or transfer of digital images / videos and ensure I only save photographs and videos of children and staff on the appropriate system or staff-only drive within school.

I will only I take or publish images of staff and students with their permission and in accordance with the school's policy on the use of digital / video images. Images published on the school website, online learning environment etc., will not identify students by name, or other personal information.

I will use the school's Learning Platform in accordance with school protocols.

I will ensure that any private social networking sites / blogs etc that I create or actively contribute to are not confused with my professional role and details of these are given to the ICT Strategy Group.

I will ensure, where used, I know how to use any social networking sites / tools securely, so as not to compromise my professional role.

I agree and accept that any computer or laptop loaned to me by the school, is provided solely to support my professional responsibilities and that I will notify the school of any "significant personal use" as defined by HM Revenue & Customs.

I will only access school resources remotely (such as from home) using the Learning Platform and follow data protection protocols to interact with them.

I will ensure any confidential data and data categorised as 'Protect-Level' is never removed or accessed from a device not owned by the school and is never transferred onto a personal USB stick or memory card.

I understand that data protection policy requires that any information seen by me with regard to staff or pupil information, held within the school's information management system, will be kept private and confidential, EXCEPT when it is deemed necessary that I am required by law to disclose such information to an appropriate authority.

I will alert the Child Protection lead / appropriate senior member of staff if I feel the behaviour of any child may be a cause for concern.

I understand it is my duty to support a whole-school safeguarding approach and will report any behaviour of other staff or pupils, which I believe may be inappropriate or concerning in any way, to the designated Child Protection lead.

I understand that all Internet and network traffic / usage can be logged and this information can be made available to the Headteacher and / or Safeguarding Lead on their request.

I understand that Internet encrypted content (via the https protocol), may be scanned for security and/or safeguarding purposes.

I understand that all activity on all school owned devices is monitored by Smoothwall e-safe and is active inside and outside of the school network.

I will only use any LA system I have access to in accordance with their policies.

Staff that have a teaching role: I will embed the school's on-line safety / digital literacy / counter extremism curriculum into my teaching.

Staff Acceptable User Agreement

User Signature

I agree to abide by all the points in the Acceptable Use Policy.

I understand that I have a responsibility for my own and others safeguarding and I undertake to be a 'safe and responsible digital technologies user'.

I understand that it is my responsibility to ensure that I remain up-to-date and read and understand the school's most recent online safety / safeguarding policies.

I understand that failure to comply with this agreement could lead to disciplinary action.

Signature

Date

Full Name

(printed)

Role:

Authorised Signature (Headteacher)

I approve this user to be set-up on the school systems relevant to their role

Signature

Date

Full Name

(printed)