St Angela's URSULINE SCHOOL

ONLINE SAFETY POLICY

Date of Review: March 2026

Date of Next Review: March 2028

Source(s): Every Child Matters, Working Together, KCSIE, DfE, CSE

Online Safety in St Angela's Ursuline

Overview of Policy

1. Context of the Policy

Our Mission Statement

St Angela's School is part of the Ursuline tradition, which has as its hallmark the pursuit of the highest standards possible in education. Through our curriculum and community life we seek to meet the needs of the whole person and to enable all to achieve their full potential. We offer to all the challenge of building up and living in a Catholic Christian community in which all members are equally valued. We share with St Angela a commitment to the service of young people, which will empower them to play their full part in society.

In the light of this we aim to:

- recognise and respond sensitively to the talents and needs of every student and provide the most appropriate means of developing their full potential
- Ensure that quality of opportunity is available to all
- Welcome, value and respect all who come to the school
- Provide opportunities for experiencing the fullness of Catholic life while developing a spirit of tolerance, understanding and respect for other cultures, traditions, lifestyles and faith
- Build a community based on justice and a sense of personal responsibility while acknowledging the power of healing, reconciliation and forgiveness
- Promote dialogue and co-operation with the wider community
- To develop student's ideas about the world and the communities within it through cultural literacy**.**

ICT in the 21st Century has an all-encompassing role within the lives of children and adults. New technologies are enhancing communication and the sharing of information.

As a school we are utilising Google Classroom as a learning platform both inside and outside of school. It allows us to provide blended learning in the light of the current extraordinary circumstances. Current and emerging technologies used in school and, more importantly in many cases, used outside of school by our students are identified from the student voice .

- The Internet
- Google in all its aspects
- e-mail
- Instant messaging including the use of simple web cams
- Blogs (an on-line interactive diary)
- Podcasting (radio / audio broadcasts downloaded to computer or MP3/4 player)
- Social networking sites for example kik, snapchat, Instagram, twitter, tiktok and facebook
- Video broadcasting sites (for example www.youtube.com, vine,)
- Chat Rooms (See NSPCC / NOS for up to date information as constantly evolving)
- Music download sites (Popular http://www.apple.com/itunes/ http://www.napster.co.uk/)
- Mobile phones / Smartphone / devices with camera and video functionality and web functionality
- Mobile technology (e.g. games consoles) that are 'internet ready'.

- Shopping and banking websites

Our Statutory Responsibilities

*'*The Internet and related technologies are powerful tools, which open up new prospects for communication and collaboration. Education is embracing these new technologies as they bring with them fresh opportunities for both teachers and learners. To use these technologies effectively requires an awareness of the benefits and risks, the development of new skills, and an understanding of their appropriate and effective use both in and outside of the classroom." ***DCFS, eStrategy***

The Green Paper ***Every Child Matters,*** the provisions of the ***Children Act 2004 Working Together to Safeguard Children and The Keeping Children Safe in Education 2024*** sets out how organisations and individuals should work together to safeguard and promote the welfare of children.

The 'staying safe' outcome includes aims that children and young people are:

- safe from maltreatment, neglect, violence,sexual and criminal exploitation
- safe from accidental injury and death
- safe from Peer on peer abuse, bullying and discrimination
- safe from crime and anti-social behaviour in and out of school
- secure, stable and cared for
- safe from FGM
- safe from Missing Education
- safe from child exploitation
- safe from radicalisation
- safe from gangs

Much of these aims apply equally to the 'virtual world' that children and young people will encounter whenever they use ICT in its various forms.

The use of technology has become a significant component of many safeguarding issues. Child sexual exploitation; radicalisation; sexual predation: technology often provides the platform that facilitates harm. An effective approach to online safety empowers a school or college to protect and educate the whole school community in their use of technology and establishes mechanisms to identify, intervene in, and escalate any incident where appropriate. The breadth of issues classified within online safety is considerable, but can be categorised into three areas of risk:

Content: being exposed to illegal, inappropriate or harmful material; for example pornography, fake news, racist or radical and extremist views;

Contact: being subjected to harmful online interaction with other users; for example commercial advertising as well as adults posing as children or young adults; and

Conduct: personal online behaviour that increases the likelihood of, or causes, harm; for example making, sending and receiving explicit images, or online bullying.

Commerce:being exposed to risks from online gambling, inappropriate advertising, phishing or financial scams

We have suitable firewalls to protect students from online targeting.

It is the duty of the school to ensure that every child in our care is safe, and the same principles apply to the 'virtual' or digital world as apply to the school's physical buildings.

This policy document is drawn up to protect all parties – the students, the staff and the school and aims to provide clear advice and guidance on how to minimise risks and how to deal with any infringements.

2.Legislation and guidance

This policy is based on the Department for Education's (DfE) statutory safeguarding guidance, Keeping Children Safe in Education, and its advice for schools on:

Teaching online safety in schools

Preventing and Tackling bullying and cyberbullying advice for head teachers and staff

Relationship and Sex education

Searching, screening and confiscation

It also refers to the Department's guidance on protecting children from radicalisation.

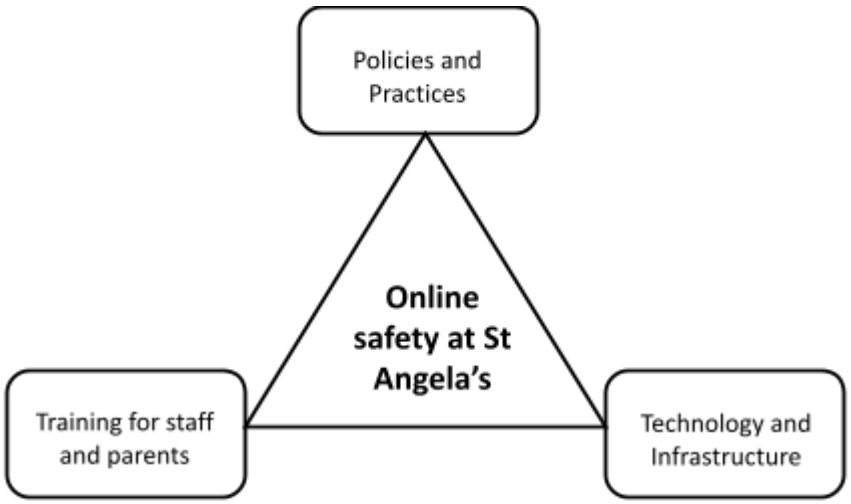
It reflects existing legislation, including but not limited to the Education Act 1996 (as amended), the Education and Inspections Act 2006 and the Equality Act 2010. In addition, it reflects the Education Act 2011, which has given teachers stronger powers to tackle cyber-bullying by, if necessary, searching for and deleting inappropriate images or files on students' electronic devices where they believe there is a 'good reason' to do so. The policy also takes into account the National Curriculum computing programmes of study.

3. Whole school approach to the safe use of ICT

St Angela's aims to:

- Have robust processes in place to ensure the online safety of students,
- Deliver an effective approach to online safety, which empowers us to protect and educate the whole school community in its use of technology
- Establish clear mechanisms to identify, intervene and escalate an incident, where appropriate.

Our safe ICT learning environment includes three main elements:



Training

- All new staff members

will receive training, as part of their induction, on safe internet use and online safeguarding issues including cyber-bullying and the risks of online radicalisation.

- All staff members will receive refresher training at least once each academic year as part of safeguarding training, as well as relevant updates as required (for example through emails, e-bulletins and staff meetings).
- The DSL and safeguarding team will undertake child protection and safeguarding training, which will include online safety, at least every 2 years. They will also update their knowledge and skills on the subject of online safety at regular intervals, and at least annually.
- Governors will receive training on safe internet use and online safeguarding issues as part of their safeguarding training.
- Volunteers will receive appropriate training and updates, if applicable.

More information about safeguarding training is set out in our child protection and safeguarding policy.

4. Roles and Responsibilities

Online safety is recognised as an essential aspect of strategic leadership in this school and the Head Teacher, with the support of Governors, aims to embed safe practices into the culture of the school. The Head Teacher ensures that the Policy is implemented and compliance with the Policy monitored. The responsibility for online safety has been designated to a member of the senior management team with safeguarding responsibilities.

Online safety coordinator/ Designated Safeguarding Lead

Our online safety coordinator/ DSL ensures they keep up to date with online safety issues and guidance through liaison with the Local Authority and through organisations such as National Online Safety, the KEY, The Child Exploitation and Online Protection (CEOP), NSPCC, Safeguarding Pro and the borough Prevent Team. In addition, the co-ordinator/ DSL will work closely with the Safeguarding team as set out in our Safeguarding and Child Protection Policy as well as relevant job description . The school's online safety coordinator will ensure that the Head, Senior Leaders and Governors are updated as necessary.

The DSL and Safeguarding Team are responsible for:

- Supporting the Headteacher in ensuring that staff understand this policy and that it is being implemented consistently throughout the school
- Working with the Headteacher and other staff, as necessary, to address any online safety issues or incidents
- Ensuring that any online safety incidents are logged as per our school behaviour policy and dealt with appropriately in line with this policy.
- Ensuring that any incidents of cyberbullying are logged on SIMs and dealt with appropriately in line with the school Behaviour, Anti Bullying policy, Safeguarding and Child Protection policies
- Updating and delivering staff training on online safety
- Liaising with other agencies and/or external services if necessary
- Providing regular reports on online safety in school to the Headteacher and/or governing board as required.

This list is not intended to be exhaustive.

The school along with the ICT Managed Service provider is responsible for:

- Putting in place appropriate filtering and monitoring systems, which are updated on a regular basis and keep students safe from potentially harmful and inappropriate content and contact online while at school, including terrorist and extremist material
- Ensuring that the school's ICT systems are secure and protected against viruses and malware, and that such safety mechanisms are updated regularly
- Conducting a monitoring check of the school's ICT system use on a fortnightly basis
- Blocking access to potentially dangerous sites and, where possible, preventing the downloading of potentially dangerous files
- Working with the Headteacher, safeguarding team, contractors and other staff, as necessary, to address any online safety issues or incidents
- Ensuring that any online safety incidents are logged as per our school behaviour policy and dealt with appropriately in line with this policy.
- Ensuring that any incidents of cyberbullying are logged and and dealt with appropriately in line with the school's Behaviour, Anti Bullying and Safeguarding and Child Protection policies

This list is not intended to be exhaustive.

Governors
Governors need to have an overview / understanding of online safety issues and strategies at this school. We ensure our governors are aware of our local and national guidance on online safety and are updated at least annually on policy developments. The governing body has overall responsibility for monitoring this policy and holding the Headteacher to account for its implementation.The governing body will coordinate regular meetings with appropriate staff to discuss online safety. The DSL/ senior member of staff with responsibility for online safety will make governors aware of the online safety monitoring procedures and logs.

We have an Online Safety Link Governor.

All governors will:
Ensure that they have read and understand this policy.
Agree and adhere to the terms of acceptable use of the school ICT systems and the internet (Appendix 3)

Staff and volunteers

All staff, including contractors and agency staff, and volunteers are responsible for:

- Maintaining and understanding of this policy,
- Implementing this policy consistently,
- Agreeing and adhering to the terms on acceptable use of the schools ICT systems and the internet (Appendix 2)
- Working with the DSL and safeguarding team to ensure any online safety incidents are logged and dealt with appropriately in line with this policy
- Ensuring any incidents of cyber- bullying are dealt with with appropriately in line with the school's Behaviour, Anti Bullying policy, Safeguarding and Child Protection Policies
- Promoting and supporting safe behaviours and following school online safety procedures.

This list is not intended to be exhaustive

Central to this is fostering a 'No Blame' and Listening School culture so students feel able to report any bullying, abuse or inappropriate materials.

All staff (both teaching and support staff) should be familiar with the school's policy including:

- Safe use of e-mail
- Safe use of Internet including use of internet-based communication services, such as instant messaging and social network
- Safe use of school network, equipment and data
- Safe use of digital images and digital technologies, such as mobile phones and digital cameras
- publication of student information/photographs and use of website
- eBullying / Cyber Bullying procedures
- Their role in providing online safety education for students
- Reporting mechanisms for raising concerns

Staff will be reminded / updated about online safety matters at least once a year. Staff must understand that there are rules for information systems misuse. If a member of staff is concerned about any aspect of their ICT use in school, they should discuss this with their line manager to avoid any possible misunderstanding.

Should a member of staff have a concern regarding a student's use if ICT, they should report this concern as appropriate through the behaviour management systems of the school or the school safeguarding systems in a timely manner so that the concern can be picked up before the end of the school day.

- Staff should be aware that Internet traffic is monitored and can be traced to the individual user. Discretion and professional conduct are essential.
- Staff that manage filtering systems or monitor ICT use will be supervised by senior management and have clear procedures for reporting issues.
- Staff training in safe and responsible Internet use and on the school Online Safety Policy will be provided as required and is included as part of the induction programme for new staff as set out in KCSIE *2025*

Staff members using a work device outside school must not install any unauthorised software on the device and must not use the device in any way which would violate the school's terms of acceptable use.

Staff must ensure that their work device is secure and password-protected, and that they do not share their password with others. They must take all reasonable steps to ensure the security of their work device when using it outside school. Any USB devices containing data relating to the school must be encrypted.

If staff have any concerns over the security of their device, they must seek advice from the school.

Work devices must be used solely for work activities.

Students

We will include online safety in the curriculum and ensure that every student has been educated about safe and responsible use, knows how to control and minimise online risks and how to report a problem. All students will sign the **Appropriate Use Charter for Students (Appendix 1). A copy of this is in the student planners** . It will be discussed at the admissions interview in both Year 7 and Year 12. School online safety policy will be discussed and approved by the Student Council. Online safety will feature in both ICT and Rise Up (PSHE) curricula.

Students are reminded that their usage of school ICT systems are monitored to safeguard themselves and others. They are expected to conduct themselves online according to the School's behaviour policy and should uphold the same high standards of respect in terms of their interactions.

Students will be taught about online safety as part of the curriculum:

The text below is taken from the National Curriculum computing programmes of study.

Relationships and sex education and health education in secondary schools
This new requirement includes aspects about online safety.

In **Key Stage 3**, students will be taught to:
Understand a range of ways to use technology safely, respectfully, responsibly and securely, including protecting their online identity and privacy
Recognise inappropriate content, contact and conduct, and know how to report concerns

Students in **Key Stage 4** will be taught:
To understand how changes in technology affect safety, including new ways to protect their online privacy and identity
How to report a range of concerns

*By the **end of secondary school**, they will know:*

- *Their rights, responsibilities and opportunities online, including that the same expectations of behaviour apply in all contexts, including online*
- *About online risks, including that any material someone provides to another has the potential to be shared online and the difficulty of removing potentially compromising material placed online*
- *Not to provide material to others that they would not want shared further and not to share personal material which is sent to them*
- *What to do and where to get support to report material or manage issues online*
- *The impact of viewing harmful content*
- *That specifically sexually explicit material (e.g. pornography) presents a distorted picture of sexual behaviours, can damage the way people see themselves in relation to others and negatively affect how they behave towards sexual partners*
- *That sharing and viewing indecent images of children (including those created by children) is a criminal offence which carries severe penalties including jail*
- *How information and data is generated, collected, shared and used online*
- *How to identify harmful behaviours online (including bullying, abuse or harassment) and how to report, or find support, if they have been affected by those behaviours*

The safe use of social media and the internet will also be covered in other subjects where relevant.

The school will use assemblies and RISE UP days to raise students' awareness of the dangers that can be encountered online and may also invite speakers to talk to students about this

Parents/ carers
St Angela's school will raise parents' awareness of internet safety in letters or other communications home, and in information via our website. We are members of National Online Safety This policy will also be shared with parents via our school website and discussed at induction.There will be regular communication home about online safety.

If parents have any queries or concerns in relation to online safety, these should be raised in the first instance with the headteacher and/or the DSL.

We will ensure that every effort is made to engage with parents over online safety matters and that parents/carers have signed and returned the **Appropriate Use Charter.**

Internet use in students' homes is increasing rapidly. Unless parents are aware of the dangers, students may have unrestricted access to the Internet. The school may be able to help parents plan appropriate supervised use of the Internet at home.

- Internet issues will be handled sensitively, and parents will be advised accordingly.
- A partnership approach with parents will be encouraged. This includes parent surveys (taken at parents' evenings from time to time to ascertain level of familiarity with what their children do online and how many hours they spend either supervised or not) and the induction evenings with demonstrations and suggestions for safe home Internet use.

Parents/carers are expected to:
Notify a member of staff or the headteacher of any concerns or queries regarding this policy
Ensure their child has read, understood and agreed to the terms on acceptable use of the school's ICT systems and internet
Parents/carers can seek further guidance on keeping children safe online from the following organisations and websites:

- What are the issues? - UK Safer Internet Centre
- Hot topics - Childnet International
- Parent factsheet - Childnet International

Visitors and members of the community

Visitors and members of the community who use the school's ICT systems or internet will be made aware of this policy, when relevant, and expected to read and follow it. If appropriate, they will be expected to agree to the terms on acceptable use .

5. Complaints / concerns regarding online safety
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. Sanctions available include:

- interview/counselling by tutor /HOY / DSL/Senior leader/ Headteacher
- informing parents or carers
- removal of Internet or computer access for a period, [which could ultimately prevent access to files held on the system, including examination coursework]
- referral to LA / Police
- Triage/ Channel referral

Our online safety coordinator / DSL oversees complaints, but some parents might raise issues via Form Tutors, or HOYs, in which case those members of staff would refer the matter on to the appropriate member of SLT (Deputy for Behaviour / online safety coordinator / DSL) .

Any complaint about staff misuse, including supply staff, must be referred to the Headteacher.

Complaints of cyberbullying are dealt with in accordance with our Behaviour, Anti-Bullying and Safeguarding and child protection Policies, as appropriate .

Where a student misuses the school's ICT systems or internet, we will follow the procedures set out in our policies on Behaviour , Mobile Devices and our Acceptable Use Charter. The action taken will depend on the individual circumstances, nature and seriousness of the specific incident, and will be proportionate.

Where a staff member misuses the school's ICT systems or the internet, or misuses a personal device where the action constitutes misconduct, the matter will be referred to the Headteacher and dealt with in accordance with the staff disciplinary procedures/staff code of conduct. The action taken will depend on the individual circumstances, nature and seriousness of the specific incident.

The school will consider whether incidents which involve illegal activity or content, or otherwise serious incidents, should be reported to the police.

Monitoring arrangements
The Deputy Head for Behaviour monitors behaviour and works in conjunction with the DSL and safeguarding team when and if safeguarding issues arise online. This policy will be reviewed every two years or if deemed necessary by the Designated Safeguarding lead . At every review, the policy will be shared with the governing board.

6. Cyber-bullying

Definition

Cyber-bullying takes place online, such as through social networking sites, messaging apps or gaming sites. Like other forms of bullying, it is the repetitive, intentional harming of one person or group by another person or group, where the relationship involves an imbalance of power. (See also the school Safeguarding and Child Protection and Behaviour policy.)

Preventing and addressing cyber-bullying

To help prevent cyber-bullying, we will ensure that students understand what it is and what to do if they become aware of it happening to them or others. We will ensure that students know how they can report any incidents and are encouraged to do so, including where they are a witness rather than the victim.

The school will actively discuss cyber-bullying with students, explaining the reasons why it occurs, the forms it may take and what the consequences can be. Pastoral teams will discuss cyber-bullying with their tutor groups, and the issue will be addressed in assemblies and through PSHE via our RISE UP days.

Teaching staff are also encouraged to find opportunities to use aspects of the curriculum to cover cyber-bullying. This includes Rise up days and Retreats where personal, social, health and economic (PSHE) education are covered , and other subjects where appropriate.

All staff, governors and volunteers (where appropriate) receive training on cyber-bullying, its impact and ways to support students, as part of safeguarding training (see section 11 for more detail).
The school also sends information/leaflets on cyber-bullying to parents so that they are aware of the signs, how to report it and how they can support children who may be affected. In relation to a specific incident of cyber-bullying, the school will follow the processes set out in the school behaviour policy . Where illegal, inappropriate or harmful material has been spread among students, the school will use all reasonable endeavours to ensure the incident is contained. The DSL will consider whether the incident should be reported to the police if it involves illegal material, and will work with external services if it is deemed necessary to do so.

Examining electronic devices

School staff have the specific power under the Education and Inspections Act 2006 (which has been increased by the Education Act 2011) to search for and, if necessary, delete inappropriate images or files on students' electronic devices, including mobile phones, iPads and other tablet devices where they believe there is good reason to do so.When deciding whether there is a good reason to examine or erase data or files on an electronic device, staff must reasonably suspect that the data or file in question has been, or could be, used to:

- cause harm and /or
- disrupt teaching and/ or
- break any of the school rules

If inappropriate material is found on the device, it is up to the staff member in conjunction with the DSL or other member of the senior leadership team to decide whether they should:

- Delete that material, or
- Retain it as evidence (of a criminal offence or a breach of school discipline), and/or
- Report it to the police
- Any searching of students will be carried out in line with the DfE's latest guidance on screening, searching and confiscation.

Any complaints about searching for or deleting inappropriate images or files on students' electronic devices will be dealt with through the school complaints procedure.

8. Acceptable use of the internet in school

All students, parents, staff, volunteers and governors are expected to sign an agreement regarding the acceptable use of the school's ICT systems and the internet . Visitors will be expected to read and agree to the school's terms on acceptable use if relevant.

Use of the school's internet must be for educational purposes only, or for the purpose of fulfilling the duties of an individual's role. We will monitor the websites visited by students, staff, volunteers, governors and visitors (where relevant) to ensure they comply with the above.
More information is set out in the acceptable use agreements in appendices 1, 2 and 3.

9. Students using mobile devices in school
- please refer to our Mobile Devices Policy

10. E-mail at St Angela's
Student email is monitored and accountable. Use may also be restricted to approved addresses and filtered for unsuitable content and viruses. This is the first line of defence. In common with other schools in London St Angela's uses an internet-based e-mail system.

This must be used for **all** communication between staff and students. All email addresses are @stangelas-ursuline.co.uk.

Procedures:
In the school context, e-mail should not be considered private and the school reserves the right to monitor email. There is a balance to be achieved between monitoring to maintain the safety of students and the preservation of human rights, both of which are covered by recent legislation.

The use of personal email addresses, such as Hotmail, must be avoided by all working in schools. Staff are required to use appropriate email systems for professional purposes.

Individual student school email addresses allow students to send and receive messages from the wider world and must be used with an understanding that the communication is monitored.

Email must not be used by staff to transfer information about students – unless it is within an encrypted, secured email system. The data (in emails or other systems) does not belong to the user but to the organisation and they are not authorised to do as they please with the organisation's data. Therefore a school user could be personally liable for breaching the Data Protection Act (DPA98) and GDPR if personal information was disclosed because of their unauthorised actions.

In St Angela's

- We use anti-virus and additional email spam, phishing software managed by our ICT management company.
- Accounts are managed effectively, with up to date account details of users.
- Messages relating to or in support of illegal activities will be reported to the relevant Authority and Police.
- If one of our staff or students receives an e-mail that we consider is particularly disturbing or breaks the law we will contact the Police.

11. Safeguarding our students

- We use communication tools within the 'closed' Learning Platform (G Suite) with the students for communication with staff and other students. All this is audited.
- Students can only use the school domain email accounts on the school system.
- Students are introduced to, and use email as part of the Computer Science scheme of work.
- Students are taught about the safety and 'etiquette' of using email both in school and more generally (for example personal accounts set-up at home) i.e.
    - not to give out their email address unless it is part of a school managed project or 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 email 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 email, such as address, telephone number, etc;
    - to not open attachments unless sure the source is safe;
    - the sending of multiple or large attachments should be limited;
    - personal information should not be sent as attachments on open email. A secure method of encrypted transfer should always be used;
    - embedding adverts is not allowed;
    - that they must immediately tell a teacher / responsible adult if they receive an email which makes them feel uncomfortable, is offensive or bullying in nature;
    - not to respond to malicious or threatening messages;
    - not to delete malicious of threatening emails, 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' email letters is not permitted.
- Students sign the school Acceptable Use Charter to say they have read and understood the online safety rules, including email and we explain how any inappropriate use will be dealt with.

Staff:

- Staff use school email systems for professional purposes
- Staff are allowed to only use the school domain email accounts on the school system;
- We never use standard email to transfer staff or student level data. We use secure, approved systems. These systems are industry standard, high level encryption with 2 factor authentication.
- We block access to external personal email accounts in school. We do not allow staff to access personal email during the school day;
- **Staff know that email 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 and that it should follow the school 'house-style'**

- the sending of multiple or large attachments should be limited
- personal information must not be sent as attachments on open email. A secure method of encrypted transfer should always be used.
- the sending of chain letters is not permitted;
- embedding adverts is not allowed;

12. Using the school network, equipment and data safely
The computer system / network is owned by the school and is made available to students to further their education and to staff to enhance their professional activities including teaching, research, administration and management.

The school reserves the right to examine or delete any files that may be held on its computer system (including online data storage) or to monitor any internet or email activity on the network.

To ensure the network is used safely St Angela's:

- Ensures staff read and sign that they have understood the school's online safety Policy. Following this, they are set-up with Internet and email access and can be given an individual network log-in username and password;
- Provides students with an individual network log-in username.
- Makes it clear that staff must keep their log-on username and password private and must not leave them where others can find;
- Makes clear that students should never be allowed to log-on or use teacher and staff logins – these have far less security restrictions and inappropriate use could damage files or the network;
- Makes clear that no one should log on as another user.
- Has set-up the network with Google Drive/Google Classroom and shared work areas for students and 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 switch the computers off at the end of the day.
- Has set-up the network so that users cannot download executable files / programmes;
- Has blocked access to music download or shopping sites – except those approved for educational purposes;
- Scans all mobile equipment with anti-virus / spyware before it is connected to the network;
- Makes clear that staff are responsible for ensuring that all equipment that goes home has the anti-virus and spyware software maintained up-to-date and the school provides them with a solution to do so;
- Makes clear that staff are responsible for ensuring that any computer or laptop 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.
- Reviews the school ICT systems regularly with regard to security.

Staff

All staff use of ICT systems including ICT equipment owned by the school falls under this policy and the Acceptable Use Charter within.

Any misuse of the ICT systems or failure to safeguard students by staff in their use of ICT systems falls under the CES Disciplinary Policy. In serious cases that policy cites under the possible actions considered gross misconduct as:

Misuse of the School's ICT (including internet and email access and breaches of the School's social networking policy) to view or distribute obscene, pornographic, defamatory or otherwise unacceptable material

The school's approach to social networking policy lies within this policy.

If a child sexual abuse image (s) are found

In the case of child sexual abuse images being found, the member of staff will be **immediately suspended** and the Police must be contacted.

The school will also report to the Local Authority Designated Officer (See Safeguarding and Child Protection policy/ https://www.newham.gov.uk/children-families/safeguarding-children/2) .

Anyone may report any inappropriate or potentially illegal activity or abuse with or towards a child online to the Child Exploitation and Online Protection (CEOP)
https://www.ceop.police.uk/safety-centre/

Other Safeguarding actions:

- Remove the PC/ Device used to a secure place to ensure that there is no further access to it.
- Instigate an audit of all ICT equipment by an outside agency, such as the schools ICT managed service providers - to ensure there is no risk of students accessing inappropriate materials in the school.
- Identify the precise details of the material.

14. Use of digital and video images and the developing of a safe school website

Our school website is an important, public-facing communication channel. Many prospective and existing parents find it convenient to look at the school's website for information and it is an effective way to share the school's good practice and promote its work. Procedures and practice need to ensure website safety.

Use of still and moving images

We ensure that we follow the GDPR policy. We take great care when using photographs or video footage of students on the school website. We use group photographs rather than photos of individual children. We do not use the names of the individuals in a photograph.

- **If the student is named, we do not use their photograph / video footage.**
- **If the photograph /video is used, we do not name the student.**

Parental permission is obtained before publishing any photographs, video footage etc of students on the school website, in a DVD or in any public printed media. We use a Parental Permission Form to ensure this on each occasion.

Links to any external websites are thoroughly checked before inclusion on our school website to ensure that the content is appropriate both to the school and for the intended audience.

In St Angela's:

- The Headteacher takes overall editorial responsibility to ensure that the websites content is accurate and quality of presentation is maintained;
- The school website complies with the school's 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;
- The point of contact on the web site is the school address and telephone number. Home information or individual email identities will not be published;
- Photographs published on the web do not have full names attached;
- 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;
- Digital images /video of students are stored in the teachers' shared images folder on the network and images are deleted at the end of the year – unless an item is specifically kept for a key school publication;
- We do not use students' names when saving images in the file names or in the <ALT> tags when publishing to the school website;
- We do not include the full names of students in the credits of any published school produced video materials / DVDs;
- Staff sign the school's Acceptable Use Charter and this includes a clause on the use of mobile phones / personal equipment for taking pictures of students;
- Students are only able to publish to their own area of the google drive / Google classroom where only associated staff can see what has been published.
- Students are taught 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 taught about how images can be abused in their online safety education programme;

15. Social networking and personal publishing

Parents and teachers need to be aware that the Internet has online spaces and social networks which allow individuals to publish unmediated content. Social networking sites can connect people with similar or even quite different interests. Guests can be invited to view personal spaces and leave comments, over which there may be limited control.

For use by responsible adults, social networking sites provide easy to use, free facilities; although often advertising intrudes and may be dubious in content. Students should be encouraged to think about the ease of uploading personal information and **the impossibility of removing an inappropriate photo or address once published.**

- St Angela's will block access to social networking sites except for educational purposes within lessons.
- Newsgroups will be blocked unless a specific use is approved.
- Students will be advised never to give out personal details of any kind which may identify them and / or their location. Examples would include real name, address, mobile or landline phone numbers, school attended, IM and e-mail addresses, full names of friends, specific interests and clubs etc.
- Students will be advised not to place personal photos on any social network space. They should consider how public the information is and consider using private areas. Advice should be given regarding background detail in a photograph which could identify the student or his/her location eg. house number, street name or school.
- Teachers' official blogs or wikis should be password protected and run from the school website. Teachers should be advised not to run social network spaces for student use on a personal basis.
- Students should be advised on security and encouraged to set passwords, deny access to unknown individuals and instructed how to block unwanted communications. Students should be encouraged to invite known friends only and deny access to others.
- Students should be advised not to publish specific and detailed private thoughts.
- Students and staff should be aware that bullying can take place through social networking especially when a space has been set up without a password and others are invited to see the bully's comments- individuals must take steps to ensure that their accounts are private .
- On starting at the school all students must read and sign Appendix 1 'Acceptable use charter for the protection of my Digital Footprint'. This can also be found in the student planner.
- On approval of this policy all stakeholders will be expected to read and sign Appendix 2 or 3 as appropriate.

16. Links with other policies

This online safety policy is linked to our:

- Safeguarding and Child Protection policy
- Behaviour policy
- Anti Bullying policy
- Staff disciplinary procedures
- Data protection policy and privacy notices
- Complaints procedure
- Mobile devices policy

17. Cyber safety at St Angela's

St Angela's in consultation with the ICT provider for the school (currently CSE) works to ensure cyber safety of all school records and resources. The principles of cyber safety are based on the DfE **Cyber security standards for schools and colleges** And following advice from the National Cyber Security Centre: Cyber Essentials.

Cyber incidents and attacks have significant operational and financial impacts on schools and colleges. These incidents or attacks will often be an intentional and unauthorised attempt to access, change or damage data and digital technology. They could be made by a person, group, or organisation outside or inside the school or college and can lead to:

- safeguarding issues due to sensitive personal data being compromised
- impact on student outcomes
- a significant data breach
- significant and lasting disruption, including the risk of repeated future cyber incidents and attacks, including school or college closure
- financial loss
- reputational damage

St Angela's Ursuline School will ensure that security measures are in place including:

- Firewalls and network security controls
- Anti-virus and anti-malware software on all devices
- Regular software updates and patch management
- Secure data backup and tested recovery procedures
- Encryption for sensitive and personal data
- Multi-factor authentication (MFA) for critical systems and remote access
- Secure configuration and monitoring of cloud services (e.g., Office 365, Google Workspace).
- Prompt removal of access for leavers

Additional precautions include

- Staff training (annually) on the principles and actions related to cyber safety
- Registry with the Police Cyber Alarm
- Addition of cyber incident recovery to St Angela's Work Continuity Plan

- **APPENDIX 1**

Acceptable Use Charter for the Protection of My Digital Footprint

I understand that I have a **digital footprint** and that information from it can be searched; copied and passed on; seen by a large, invisible audience, which will always be there.

In line with the **School's Mission Statement and the Home School agreement** which I signed when I started at St Angela's, I have a r**esponsibility** to be **respectful** to others and understand what can be done to keep myself and others safe.

I recognise that people's online **information can be helpful or harmful** to their **reputation** and image.

I have a responsibility to protect my reputation and that of friends and family and the communities I am part of by:

- ➢ Protecting my Passwords
- ➢ Not sharing personal information about myself and other people
- ➢ Checking my privacy settings regularly
- ➢ Never reposting* negative comments or images
- ➢ Never passing on other peoples posts* without their permission
- ➢ Remembering 'Stranger Danger' still applied online
- ➢ Understanding that posting hurtful comments, threats and certain images is breaking the law
- ➢ Using the report abuse button if I think something may cause harm to a person's feelings, reputation or safety
- ➢ Letting an adult know if I have any worries or concerns about this
- ➢ Always thinking of my reputation and the effect my actions could have on my friends, family and community

The term 'post' refers to all comments , tweets, images, texts etc made on Social networks & mobile phones

Signed : . . . . . *(Student)*

*(Print Name)*_____

Signed : . . . . . *(Parent)*

*(Print Name)*_____

This Acceptable Use Charter has been drawn up in consultation with the students, staff and Governors of St Angela's School

Appendix 2:

ACCEPTABLE USE OF THE SCHOOL'S ICT SYSTEMS AND INTERNET: AGREEMENT FOR STUDENTS AND PARENTS/CARERS	
Name of student:	
I will read and follow the rules in the acceptable use agreement policy. **I understand that I will be using Google classroom as part of my education. I understand that the same expectations and code of conduct apply to the use of Google classrooms and emails as to my everyday behaviour choices.** **When I use the school's ICT systems (computers / chrome book) and access the internet at school I will:** ● Always use the school's ICT systems and the internet responsibly and for educational purposes only ● Only use them when a teacher is present, or with a teacher's permission ● Keep my username and passwords safe and not share these with others ● Keep my private information safe at all times and not give my name, address or telephone number to anyone without the permission of my teacher or parent/carer ● Tell a teacher (or sensible adult) immediately if I find any material which might upset, distress or harm me or others ● Always log off or shut down a computer when I'm finished working on it **I will not:** ● Access any inappropriate websites including: social networking sites, chat rooms and gaming sites unless my teacher has expressly allowed this as part of a learning activity ● Open any attachments in emails, or follow any links in emails, without first checking with a teacher ● Use any inappropriate language when communicating online, including in emails ● Log in to the school's network using someone else's details ● Arrange to meet anyone offline without first consulting my parent/carer, or without adult supervision **If I bring a personal electronic device into school:** ● I will not use it during lessons, tutor group time, clubs or other activities organised by the school, without a teacher's permission ● I will use it responsibly, and will not access any inappropriate websites or other inappropriate material or use inappropriate language when communicating online **I agree that the school will monitor the websites I visit and that there will be consequences if I don't follow the rules.** **I am aware that the school will monitor the emails and communications I send and there will be consequences if my code of conduct is not appropriate**	
Signed (student):	**Date:**
Parent/carer's agreement: I agree that my child can use the school's ICT systems and internet when appropriately supervised by a member of school staff.I agree that my child can use a chrome book or other device at home for educational purposes and i will play my part in ensuring my child's safety online. I agree to the conditions set out above for students using the school's ICT systems and internet, and for using personal electronic devices in school, and will make sure my child understands these.	
Signed (parent/carer):	**Date:**

Appendix 3:

ACCEPTABLE USE OF THE SCHOOL'S ICT SYSTEMS AND INTERNET: AGREEMENT FOR STAFF, GOVERNORS,VOLUNTEERS AND VISITORS	
Name of staff member/governor/volunteer/visitor:	
When using the school's ICT systems and accessing the internet in school, or outside school on a work device (if applicable), I will not: ● Access, or attempt to access inappropriate material, including but not limited to material of a violent, criminal or pornographic nature (or create, share, link to or send such material) ● Use them in any way which could harm the school's reputation ● Access social networking sites or chat rooms ● Use any improper language when communicating online, including in emails or other messaging services ● Install any unauthorised software, or connect unauthorised hardware or devices to the school's network ● Share my password with others or log in to the school's network using someone else's details ● Use mobile phones / personal equipment for taking pictures of students; ● Take photographs of students without checking with the DSL/ Senior leadership team first ● Share confidential information about the school, its students or staff, or other members of the community ● Access, modify or share data I'm not authorised to access, modify or share ● Promote private businesses, unless that business is directly related to the school	
I will only use the school's ICT systems and access the internet in school, or outside school on a work device, for educational purposes or for the purpose of fulfilling the duties of my role. I agree that the school will monitor the websites I visit and my use of the school's ICT facilities and systems. I will take all reasonable steps to ensure that work devices are secure and password-protected when using them outside school, and keep all data securely stored in accordance with this policy and the school's data protection policy. **I will let the designated safeguarding lead (DSL) know if a student informs me they have found any material which might upset, distress or harm them or others, and will also do so if I encounter any such material**. I will always use the school's ICT systems and internet responsibly, and ensure that students in my care do so too.	
For staff delivering lessons : **If circumstances necessitate a requirement to teach online lessons, I will ensure nothing inappropriate can be seen or heard in the background.** **I understand that online teaching online differs from teaching face-to-face in a classroom, and that I must always maintain the same high professional relationships with the students in this forum, as outlined in both our Behaviour Policy and Safeguarding and Child Protection Policy.** **I understand our Acceptable Use Policy and Behaviour Policy has clear expectations about what behaviour is acceptable for both teachers and students in the online teaching forum.** **Should I have a concern regarding a student during online teaching, I will report this concern as appropriate through the behaviour management systems of the school or the school safeguarding systems in a timely manner so that the concern can be picked up before the end of the school day**	
Signed (staff member/governor/volunteer/visitor):	**Date:**