WELLING SCHOOL

E-SAFETY POLICY

This Policy was reviewed:

January 2023

The Policy will next be reviewed by TKAT & Welling School by:

January 2024[1]

1. Part 1: Introduction

1.1. Purpose of the Esafety Policy?

The E-safety policy document serves to identify and mitigate risk and provides us with a written set of guidelines. Digital technologies are a powerful tool, opening up new opportunities that play an integral part to the lives of young people both in and out of school. The e-safety policy is a statutory duty that must put in place by Welling School, in order to fulfil their safeguarding and wider duty of care for the children and young people in their school.

The purpose of having an E-safety Policy is important because it provides a set of guidelines for all to follow; such as:

- Ways to safeguard and protect the children and staff at Welling School and to assist school staff working with children to work safely and responsibly with the internet and other communication technologies and to monitor their own standards and practice. That staff and students are aware of the school monitoring/filtering software, and how this will be policed.
- Provide a clear and consistent framework when responding to and reporting E- safe incidents such as cyberbullying, and ensures that where problems occur, children, young people and their parents/carers, have the correct support in dealing with them in an effective manner.
- Ensure everyone responsible for the students is fully aware of his/her E-Safe responsibilities. Ensure that all members of the school community are aware that unlawful and inappropriate behaviour and exposure to inappropriate content can lead to disciplinary or legal action.
- Set boundaries of use of any school owned IT equipment, or personal IT equipment used in the school, and set the boundaries of services such as social networking (e.g. blogging, Twitter).
- Ensure staff and students are aware of the school monitoring/filtering software, and how this will be policed.

1.2. Scope of Policy

This policy applies to all members of Welling School community, including staff, pupils, volunteers, parents/carers, visitors and community users.

The Education and Inspections Act 2006 empowers Headteachers, to such extent as is reasonable, to regulate the behaviour of pupils when they are off the school site and empowers members of staff to impose disciplinary penalties for inappropriate behaviour. This is pertinent to incidents such as cyber-bullying and inappropriate use of social networking by pupils and staff, which may take place out of school, but are linked to membership of the school. It also applies to both staff and pupil use of technology for remote/online learning as part of a blended approach and during any school closures (partial or full) e.g. during a national/local lockdown or due to severe weather.

Keeping Children Safe in Education 2020 sets out specific responsibilities for governing bodies to ensure:

- children are taught about online safety
- appropriate filters and appropriate monitoring systems are in place
- online safety training for staff is integrated, aligned and considered as part of the overarching safeguarding approach

The school will manage Online Safety as described within this policy and associated behaviour and anti-bullying policies and will inform parents and carers of known incidents of inappropriate Online Safety behaviour that take place in and out of school.

This Online Safety Policy should be read in conjunction with the following other linked school policies:

- *Safeguarding and Child Protection Arrangements during school closure due to COVID-19*
- *Safeguarding Policy*
- *Bullying Policy*
- *Behaviour Amendment Policy due to COVID-19*
- *Behaviour Policy and*
- *TKAT Remote Learning Policy*

1.3. Risk Assessment

Welling School will take all reasonable care to mitigate potential risk or harm to children and young people when using technology introduced by the school. Therefore, technology device (tablets, smart phone) or services (social media) will be assessed for any foreseeable risk to the students and staff, 'for the likelihood that something may happen and the impact of it happening'. To ensure that all users can only access appropriate material, as far as is possible.

Welling School has made every effort to take all relevant laws and best practice in the preparation of this policy. However, due to the international scale and linked nature of content on the internet, the availability of mobile technology and the speed of changes it is not possible to guarantee that unsuitable material will never appear on a school computer. E-safety issues have the potential to be complex and versatile, nothing in this policy constitutes legal advice.

1.4. Disclaimer

Welling School can therefore accept NO liability for any damaged or loss suffered whether it is (directly, consequentially, indirectly, or otherwise) by anyone relying on the information in this policy.

1.5. Handling E-safety Complaints

The E-safety Co-ordinator and **Designation Safeguarding Lead (DSL)** acts as the first point of contact for matter arising from internet use, any matter of staff misuse is referred to the Headteacher.

Staff and pupils are given information about possible sanctions for handling of e-safety and e-safeguard complaint, such as:

- Interview with the safeguarding team, E-safety Co-ordinator, Headteacher and informing parents/carers, referring to Local Authority [Bexley Council], Police or other relevant authority. (See illegal and inappropriate flowcharts for reporting incidents).
- Removal of Internet access for a set period

Any complaint of Cyberbullying is dealt with in accordance with Welling School Behaviour and Anti-bullying policy, and complaints with regards to Child Protection issues are dealt with by the school safeguarding team. **Other ways of reporting online bullying are: Online bully box, Childline App and phone number 0800 1111, Professionals Online Safety Helpline (POSH) 0344 381 4772.**

Sexting

The school will follow UKCIS advice on how to respond to any incident of sexting. We will provide appropriate support for sexting incidents which take place in and out of school. Within school, any device which has an illegal image of a child under 18, or is suspected of having such an image, will be secured and switched off. This will then be reported to the Designated Safeguarding Lead (DSL). An individual member of staff will not investigate, delete or pass on the image. The Designated Safeguarding Lead (DSL) will record any incident of sexting and the actions taken in line with advice from Bexley Local Authority.

Sexual Harassment, including Upskirting

All staff are made aware that sexual harassment can occur between two children of any age and sex and can include online harassment. Online sexual harassment may be standalone, or part of a wider pattern of sexual harassment and/or sexual violence and can include:

- non-consensual sharing of sexual images and videos
- sexualised online bullying
- unwanted sexual comments and messages, including, on social media
- sexual exploitation; coercion and threats
- Upskirting

All staff are made aware of what Upskirting is, and that it is illegal. Any incident of sexual harassment will be taken seriously and reported to the Designated Safeguarding Lead (DSL). The Designated DSL will record the incident(s) and the actions taken in line with DfE Guidance and advice from Bexley Local Authority and/or the police as necessary.

Prevent

The school works to ensure children are safe from terrorist and extremist material when accessing the internet on the premises. Appropriate levels of filtering are in place through a managed filtering service which includes terms related to terrorism.
Appropriate monitoring of internet use will identify attempts to access such material. Children are educated to evaluate information accessed with a reporting procedure that identifies inappropriate sites so that action, including blocking, can be put into place

2. Part 2: Roles & Responsibilities

E-safety is the responsibility of everyone, with the ultimate responsibility resting with the Headteacher and governing body. E-safety is not an ICT issue but a safeguarding issue, and it must be treated this way. The day to day duties will be dealt with by the safeguarding and E-safety person-in -charge, who will document incident accordingly.

2.1. Headteacher

The Headteacher has overall responsibility for E-safety provision at Welling School, and as such will report to the governing body. The day to day responsibility will be delegated to the E-safety Co-ordinator, and regular monitoring report update will be received from the IT Technician where necessary.

The Headteacher will ensure:

- E-Safety training throughout the school is planned and up to date and appropriate to the recipient, i.e. students, staff, senior leadership team, governing body and parents/carers.
- That the delegated E-safety Co-ordinator will receive relevant CPD training in order to carry out their day to day duties, and to train other colleagues.
- There is correct procedure to follow in the event of a serious E-safety incident and that incidents are dealt with promptly and appropriately.

2.2. Governing Body

The governing body is accountable for ensuring that Welling School has an effective E-safety policy and procedures in place.

They will ensure that:

- E-safety policy is reviewed at least annually and in response to any e-safety incident to ensure that the policy is up to date, covering all aspects of technology use at Welling School.
- E-safety incidents reported are appropriately dealt with and the policy was effective in managing those incidents.
- The College encourages parents and the wider school community to become engaged in e-safety activities.
- One governor is appointed to have overall responsibility for the governance of E- safety at Welling School.

The E-safety governor role will include:

- Keeping up-to-date with emerging risks and threats through technology use, and Welling School follows all e-safety advice to keep staff and students safe.
- Having regular review meeting with the E-safety Co-ordinator or DSL (including any e-safety incident logs,)

2.3. E-Safety Coordinator and/or Safeguarding Lead

The E-safety Coordinator will:

- Keep up to date with the latest risks to children whilst using technology; with the latest research and available resources for school and home use.
- Review this policy regularly and bring any matters to the attention of the Headteacher.
- Advise the Headteacher and governing body on E-safety and e-safeguarding matters.

- Engage with parents and the school community on E-safety and e-safeguarding matters at school and/or at home (letters, text messages, appropriate resources on the school website)
- Liaise with the local authority, IT technical support and other agencies as required.
- Be responsible for the incident log; ensure staff and students are aware of procedure for reporting incident.
- Ensure any technical e-safety measures in school (e.g. Internet filtering software, monitoring software 'SENSO') are fit for purpose through liaising with the IT Technician.

2.4. IT Technician staff

The IT Technician is responsible for ensuring that the school network infrastructure is safe and secure and not open to misuse or malicious attack.

The following applies to the IT infrastructure at Welling School:

- Has the educational filtered secure broadband connectivity through the MLL Telecoms and so connects to the 'private' National Education Network.
- Uses the MLL Smoothwall System which blocks sites that fall into categories such as pornography, race hatred, gaming, sites of an illegal nature, etc. All changes to the filtering policy are logged and only available to staff with the approved 'web filtering management' status.
- Ensures network healthy through use of Symantec Endpoint anti-virus software and network set-up so staff and pupils cannot download executable files.
- Chat rooms and social networking sites are blocked except those that are part of an educational nature.
- Blocks pupil access to music download or shopping sites – except those approved for educational purposes.
- When applicable 'Senso' can set a user's internet to be disabled for any period of time or permanently.
- Is vigilant in its supervision of pupils' use at all times, as far as is reasonable, and uses common-sense strategies in learning resource areas where older pupils have more flexible access.
- Logon screen has the following statement – "The act of logging on indicates acceptance to the General Conditions of Use & Information Security Policy. A copy of these documents is available online and on all staff desktops".
- Please note that students are not permitted to use staff workstations, any logon by student and requests will be denied.
- Google Safe Search is enforced across all computers on the Welling School Domain.
- Informs all users that Internet use is regularly monitored, including those using Google account issued by the school e.g. for blended learning.

- Immediately refers any material suspect is illegal to the appropriate authorities – Head teacher, Police – and the LA and our ISP.

Network Management (user access and backup)

- Audited log-ins for all users is carried out by our onsite Active Directory. Creating each person an individual account to access computers and emails.
- Guest accounts occasionally for external or short term visitors for temporary access to appropriate services.
- IT Administrator password is to be changed on a monthly (60 day) basis.
- Uses teacher 'remote' management control tools for controlling workstations / viewing users / setting-up applications and Internet web sites, where useful; has additional local network auditing software installed.
- Ensures the Systems Administrator / 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; receive regular emails from LGfL with changes to services and policies.

To ensure the network is used safely, at Welling School:

- All new staff and pupils are required to read and sign that they have understood the school's e-safety AUP. Following this, they are set-up with username to access the Internet and school network. Advice is given to create strong password using a mixture of letters, number and symbols, and that password must be kept safe at all time.
- Makes clear that no one log on as another user and makes clear that pupils should never be allowed to log-on or use teacher and staff logins as these have far less security restrictions and inappropriate use could damage files or the network.
- There is a shared network area, 'Student resources' for pupils to access files and 'Staff resources' for staff to save work and access files.
- 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. Users needing access to secure data are timed out after (120) minutes and have to re-enter their username and password to re- enter the network.
- The network is set up so that users cannot download executable files / program.
- Access to music/media download or shopping sites – except those approved for educational purposes is blocked.
- NO mobile devices are allowed to connect to the school's network and NO school equipment is allowed home, or loan out by the IT department.
- Regular inspections are performed to ensure all equipment is safe. Any unsafe equipment found is removed from use.

- Ensures that remote access to the school's network resources from remote locations by staff is restricted and access is only through school. e.g. teachers access their area / staff shared area for planning documentation via a VPN solution.
- Temporary restricted users are available from outside users to use the school network.
- Provides pupils and staff with access to content and resources through the approved Learning Platform which staff and pupils access using their username and password.
- Has a clear disaster recovery system in place for critical data that includes a secure, remote back up of critical data, that complies with external Audit's requirements; all critical data is backed daily on site and off site to allow disaster recovery from any site.
- Ensures that all pupil level data or personal data sent over the Internet is encrypted or only sent within the approved secure system.
- 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; all firewalls and routers have been configured by our ISP. We have no access to make changes.
- Our wireless network has been secured to industry standard Enterprise security level /appropriate standards suitable for educational use; No wireless access is available to students. What Wi-Fi is available always uses Wi-Fi Protected Access II.
- All computer equipment is installed professionally and meets health and safety standards; and inspected and tested to meet health and safety standards.
- Projectors are cleaned and inspected for image clarity so that the quality of presentation remains high.
- The school ICT systems are regularly inspected with regard to health and safety and security, to confirm that the school's ICT security is robust enough. Any holes/lapses in the security that are found are dealt with immediately. Inspection of ICT equipment is carried out regularly to identify any items that may cause a Health and Safety issue. If any items are found they are removed from use.

2.5. All Staff

Staff should ensure:

- All details within this e-safety policy are understood. If anything is not understood, it should be brought to the attention of the Headteacher or E-safety Co-ordinators for clarification.
- That all new staff read and signs the AUP before having access to the school network.
- Any e-safety incident is reported to the E-safety Co-ordinator (and an e-safety incident report is made), or in their absence to the Headteacher. If you are unsure the matter is to be raised with the E-safety Officer, see the Headteacher to make a decision.
- The reporting flowcharts contained within this e-safety policy are fully understood.

2.6. All students /Pupils

Students and pupils will be taught:

- The boundaries for use of ICT equipment and Internet access at Welling School are given in the student Acceptable Use Policy (AUP); any misuse of ICT equipment or Internet access will be dealt with in accordance with the school behaviour policy.
- The importance for the AUP, and to know that it must be read and sign on acceptance to attend Welling School
- All material sourced online and used in their work must be acknowledged in order to respect copyright.
- E-safety activities that are embedded into the school curriculum and all students will be given the appropriate advice and guidance for how to stay safe and behave online.
- How to report e-safety issues or areas of concern whilst at school or outside of school.

2.7. Parents and Carers

Parents play an essential role in the development of their children's e-safety habits; therefore, Welling School will ensure that parents have the skills and knowledge they need to ensure the safety of children outside the school environment. This will be done through school email, text, information on the school website, or any other appropriate medium that will keep parents up to date with new and emerging e-safety risks.

On admission to Welling School, parents/carers will ask to sign the student Acceptable Use Policy before their child has access to school ICT equipment or services. Parents/carers will be asked to support these rules with their children.

2.8. The Wider Community

It is important that the wider school community is equipped with the knowledge to stay risk free whilst communicating online. Therefore, Welling School will provide opportunity for the wider community to gain e-safety knowledge available on the school website.

3. Part 3: Technical Infrastructure

3.1. Internet and Email Filtering

Welling School use Internet filtering to prevent access to illegal, inappropriate websites. This is a piece of software that prevents any infected email to be sent from the school, or to be received by the school. Infected is defined as: an email that contains a virus or script (i.e. malware) that could be damaging or destructive to data; spam email such as a phishing message.

3.2. Monitoring

The use of the Internet in school is a privilege, not a right and can be subjected to monitoring, and all staffs are reminded that emails are subject to **Freedom of Information** requests, and as such the email service is to be used for professional work-based emails only. The use of personal email addresses for work purposes is not permitted.

3.3. Encryption

All school devices that hold personal data (as defined by the Data Protection Act 1998) are encrypted. No data is to leave the school on an un-encrypted device; all devices that are kept on school property and which may contain personal data are encrypted. Any breach (i.e. loss/theft of device such as laptop or USB etc) is to be brought to the attention of the Headteacher immediately**. (Note: Encryption does not mean password protected.)**

3.4. Password

All staff are forced to change their password regularly and the system has policies in place to make sure their password contains a mixture of letters, numbers and symbols. Students are taught about what makes a strong password in their E-safety lessons. All staff and students are advised not to share their passwords with anyone.

3.5. Anti-Virus

All devices will have anti-virus software. This software will be regularly updated and the IT Technician will be responsible for ensuring this task is carried out, and will report to the Headteacher if there are any concerns.

3.6. Social Network Post

Welling School like most schools is vulnerable to inappropriate material posted online, if you are aware of anything bringing the school into disrepute you must report it to the IT Technician or Headteacher. The school will check on a regular basis using search engines to see if any such material has been posted. When using social networking sites, you are advised not to publish detailed 'personal views' relating to Welling School, other members of staff or students.

4. Part 4: Policy Document

4.1. Digital media

Photos and videos are covered in the schools' 'Children Protection and Safeguarding Policy', and is re-iterated here for clarity. The following is to be strictly adhered to:

- Permission slips (via the school photographic policy) must be consulted before any image or video of any child is uploaded.
- There is to be no identification of students using first name and surname; first name only is to be used.
- Where services are "comment enabled", comments are to be set to "moderated".
- All posted data must conform to copyright law; images, videos and other resources that are not originated by the school are not allowed unless the owner's permission has been granted or there is a license which allows for such use (i.e. creative commons).

Notice and take down policy – should it come to the school's attention that there is a resource which has been inadvertently uploaded, and the school does not have copyright permission to use that resource, it will be removed within ***one working day***.

4.2. Mobile Phone

To promote a safe working environment, avoid distraction and disruption during the working day and to reduce the risk or misuse of technology when working with children. It is advisable that staff are not permitted to call parents/carers on their personal mobile phones, unless in difficult circumstances when all other method of communication fails; then use 'settings on your phone to keep number private' or 141 code to withhold your own number before dialling.

Mobile phones should be switched off or on silent and be out of sight during lesson times. Not at any time are staff allowed to take photographs or recordings of any students on their personal mobile phone.

4.3. Data Protection

It is the responsibility of all members of Welling School to take care when handling, using or transferring personal data that it cannot be accessed by anyone who does not:

- Have permission to access that data, and/or need to have access to that data.

Data breaches can have serious effects on individuals and / or institutions concerned, can bring the Welling School into disrepute and may well result in disciplinary action, criminal prosecution and fines imposed by the Information Commissioners Office, for the school and the individuals involved. Particularly, all transfer of data is subject to risk of loss or contamination. Personal data held by Welling School will be recorded, processed, transferred and made available according to the Data Protection Act 1998

4.4. Policy Statement

For clarity, the e-safety policy uses the following terms unless otherwise stated:

Parents/Carers – any adult with a legal responsibility for the child/young person outside the school e.g. guardian, parents, carers.

School – any school business or activity conducted on or off the school site, e.g. visits, conferences, school trips etc.

Wider school community – refers to staff, governing body, school volunteers, students and any other person working in or on behalf of the school, including contractors.

Welling School will hold the minimum personal data necessary to enable it to perform its function and it will not hold it for longer than necessary for the purposes it was collected for. Every effort will be made to ensure that data held is accurate, up to date and that inaccuracies are corrected without unnecessary delay.

Safeguarding is a serious matter; at Welling School we use technology and the Internet extensively across all areas of the curriculum. Online safeguarding, known as e-safety is an area that is constantly evolving and as such this policy will be reviewed on an annual basis or in response to an e-safety incident, whichever is sooner.

The purpose of this policy is to:

- To ensure the requirement to empower the whole school community with the knowledge to stay safe and minimise online risk.
- To ensure risks are identified, assessed and mitigated (where possible) in order to reduce any foreseeability of harm to the student or liability to the school.

This policy is available for anybody to read on the school website; upon review all members of staff will read the e-safety policy and sign the Acceptable User Policy. On admission to Welling School, students Acceptable Use Policy will be sent home and upon return of the signed permission slip and acceptance of the terms and conditions, students will be permitted access to school technology including the Internet.

WELLING SCHOOL

4.5. E-safety Keyterms and Definition

Age related filtering	Differentiated access to online content managed by the school and dependent on age and appropriate need.
AUP	Acceptable Use Policy
CEOP	Child Exploitation and Online Protection centre.
Cyber bullying	Bullying using technology such as computers and smart mobile phone, to harass another person. This can cause serious effect on another person. Here at Welling School the Anti- bullying policy has strategies that deal with issues arising from cyberbullying.
Encryption	Computer program that scrambles data on devices such as laptops and memory sticks in order to make it virtually impossible to recover the original data in event of the loss of the device; schools often use this to protect personal data on portable devices.
E-safety mark	Accreditation for schools reaching threshold levels, within 360 degree safety, through assessment by external assessor.
Frape	Short for 'Facebook rape', referring to when a Facebook user's identity and profile are compromised and used by a third party to cause upset.
Games Console	Examples include XBOX 360/ONE, Nintendo Wii, PlayStation 3&4, Nintendo DS,PSP
Grooming	Online grooming is defined by the UK Home Office as: 'a course of conduct enacted by a suspected paedophile, which would give a reasonable person cause for concern that any meeting with a child arising from the conduct would be for unlawful purposes'.
Hacker	Originally thought of as a computer enthusiast, but now a hacker is normally used to refer to computer criminals, especially those who break into other people's computer networks.
ISP	Internet Service Provider (a company that connects computers to the internet for a fee).

Lifestyle website	An online site that covertly advocates particular behaviours and issues pertaining to young and often vulnerable children for example anorexia, self-harm or suicide.
Locked down system	In a locked down system almost every website has to be unbarred before a pupil can use it. This keeps the pupils safe, because they can use only websites vetted by their teachers, the technicians or by the local authority, any other website has to be unbarred for a pupil to be able to use it, which takes up time, detracts from learning and does not encourage the pupils to take responsibility for their actions (note that a locked down system may be appropriate in an EYFS setting or in a special school).
Malware	Bad software or programs that damage your computer (viruses), steal your personal information (spyware), display unwanted adverts (adware) or expose your computer to hackers (Trojan horses).
Managed system	In a managed system the school has some control over access to websites and ideally offers age-appropriate filtering. Pupils in schools that have managed systems have better knowledge and understanding of how to stay safe than those in schools with locked down systems because they are given opportunities to learn how to assess and manage risk for themselves.
Phishing	Pronounced the same as 'fishing' this is an attempt to trick people into visiting malicious websites by sending emails or other messages which pretend to come from banks or online shops; the e-mails have links in them which take people to fake sites set up to look like the real thing, where passwords and account details can be stolen..
Profile	Personal information held by the user on a social networking site.
RBC	Regional Broadband Consortium, often providers of schools broadband internet connectivity and services in England, for example SWGfL, London Grid for Learning (LGfL).

Safer Internet Day	Initiated by the European Commission and on the second day, of the second week of the second month each year.
Sexting	Sending and receiving of personal sexual images or conversations to another party, usually via mobile phone messaging or instant messaging.
SHARP	Example of an anonymous online reporting mechanism (Self Help And Reporting Process).
SNS	Social networking; not the same as computer networking, social networking is a way of using the internet and the web to find and make friends and stay in touch with people.
Spam	An e-mail message sent to a large number of people without their consent, usually promoting a product or service (also known as Unsolicited Commercial Email (UCE) or junk email).
Trojan	A malware program that is not what it seems to be. Trojan horses pretend to be useful programs like word processors but really install spyware or adware or open up a computer to hackers.
Up skirting	Upskirting refers to the act of taking a photograph (also known as a “creepshot”) of underneath a person’s skirt without their permission. Upskirting is an alarmingly common occurrence and is usually performed in a public place, which is often crowded, which makes it hard to spot people taking such images.

Part 5 - Staff - Acceptable Use Policy

Monitoring – I understand that at Welling School, all Internet and email activities will be subjected to monitoring.

Internet access/remote teaching– I understand that I must not upload, download, access or attempt to access any materials that contain any of the following: child abuse images; pornography; promoting discrimination of any kind such as racial or religious hatred; radicalisation, self-harm; or any other information which may be illegal or offensive and may cause harm or distress to others. Inadvertent access to such materials must be treated as an E-safety incident, reported to the E-safety Coordinator and an incident log is completed.

Social networking – I understand that social networks in school are used in accordance with the E-safety policy. I know I should never undermine the school, its staff, parents or students when using social networking sites for personal use. I will not engage in any on- line activity that may compromise my professional responsibilities.

Email – I am not permitted to use Welling School email addresses for personal business, as it should always be kept professional. I am aware that school data, including emails, is open to Subject Access Requests under the Freedom of Information Act. I will only email students and parents / carers using my official school email address (@wellingschool-tkat.org). Staff using Google account issued at Welling School will use it only for educational purposes and it will be subjected to monitoring via Google vault by the IT Technician.

Mobile phone - I am not permitted to call parents /carers using my own mobile phone; unless in circumstances if out on a school trip and other method of communication fails. Then I will withhold my number using 141 code, before dialling parents/carers number.
During lesson times I will ensure that my mobile phone is on silent or switched off, and out of sight, and not at any time will I take photographs or recordings of students on my personal mobile phone.

Passwords – I know it is my responsibility to keep my password private, and there is no occasion when my password needs to be shared with another member of staff, student, or IT support.

General Data Protection Regulation – If I take work home, or off site, I will ensure that any device (USB, tablets etc.) is encrypted and password protected. I know that I am not allow to take personal information offsite on an unencrypted device. I could be subjected to disciplinary action. No personal data must ever be stored on private equipment.

Images and Videos – I will not upload onto any internet site or service images or videos of myself, other staff or pupils without consent. This is applicable professionally (in school) or personally (i.e. staff outings).

Viruses and Other Malware - any virus outbreaks are to be reported to the IT Technician as soon as it is practical to do so, along with the name of the virus (if known).

Copyright – I will ensure that permission is gained to use original work of others in my own work, and when protected by copyright, I will not download or share copies (video, music, and gaming)

E-safety – I know that E-safety is the responsibility of everyone at Welling School. As such I will promote positive E-safety messages in all use of online digital communication whether I am with other members of staff or with students.

I understand that if I fail to comply with this Acceptable Use Policy Agreement, I could be subject to disciplinary action. This could include verbal/verbal warning, a suspension, referral to Governors / or the Local Authority and in the event of illegal activities the involvement of the police.

I have read and understand the above and agree to use the school IT systems (both in and out of school) within these guidelines.

NAME:

SIGNATURE: _____

DATE: _____

WELLING SCHOOL

Part 6 - Students - Acceptable Use Policy

Note: All Internet and email activities will be subjected to monitoring

I Promise…

- To only use WELLING SCHOOL internet access or network systems and Google account for schoolwork that my teacher has asked me to complete, for educational purposes only
- Not to research, look for or show other people things that may be upsetting or offensive.
- To show respect for the work that other people have done.

I will not …

- Use other people's work or images without permission to do so (copyright & plagiarism).
- Damage the ICT equipment e.g. monitor, keyboard, mouse or other computer hardware.
- Remove or change software, create or upload viruses, deliberate deletion of files or unauthorised configuration.
- Share my password with anybody, and if I forget my password I will let my teacher know.
- Use other people's usernames or passwords, or share personal information online with anyone.
- Download anything from the Internet unless my teacher has asked me to.
- Use my Google account to transmit anything that may deem offensive e.g. racial, sexual, religious or any other illegal activities.

I will…

- Let my teacher know if anybody asks me for personal information.
- Let my teacher know if anybody says or does anything to me that is hurtful or upsets me.
- Be respectful to everybody online; I will treat everybody the way that I want to be treated (etiquette).

I understand…

- That some people on the Internet are not who they say they are, and some people can be nasty. I will tell my teacher if I am ever concerned in school or my parents if I am at home.
- If I break the rules in this charter, there will be consequences of my actions and my parents will be told.

- WELLING SCHOOL mobile phone policy, if you choose to bring a mobile device into school it should be switched off and remained switch off whilst on the School site.
- That my Google account will be regularly monitored for inappropriate material e.g. cyberbullying, swearwords etc.

I understand that I am responsible for my actions, both in and out of school…

- I understand that WELLING SCHOOL has the right to take action against me if I am involved in incidents of inappropriate behaviour, that are covered in this agreement, (example cyber-bullying, use of images or personal information).
- If I fail to comply with this Acceptable Use Policy Agreement, I will be subject to WELLING SCHOOL behaviour policy such as loss of access to the school network / internet, Google account, detentions, suspensions, my parents/carers informed and in the event of illegal activities involvement of the police.

I have read, discussed and understood the above guidelines with my son/daughter.

Tutor Group: _____

Parent/Carer: _____

Signed: _____Date: _____

Student: _____

Signed: _____Date: _____

Part 7 - Other E-safety documents

Why we filter the Internet?

Whilst sometimes seen as one of the more frustrating IT services in schools, Internet filtering is one item in the e-safety toolbox that is of particular importance. When talking about an Internet filter there are two important aspects:

Broadly Speaking

Filtering - this is a proactive measure to ensure safety (as much as possible) or prevent users from accessing illegal or inappropriate (by age) websites.

Monitoring - this is a reactive measure and for the most part means searching, browsing or interrogating filter logs (known as the cache) for Internet misuse.

Why Do We Filter and Monitor?

Welling School filters Internet activity for two reasons:

- We filter to ensure: That (as much as possible) that children and young people and adults are not exposed to illegal or inappropriate websites. These sites are (or should be) restricted by category dependent on the age of the user. Exposure would include browsing to specifically look for such material, or as a consequence of a search that returns inappropriate results.
- That as much as possible that the school has mitigated any risk to the children and young people, and thereby reduces any liability to the school by making reasonable endeavours to ensure the safety of those children and young people.
- We monitor for assurance: That [as much possible] no inappropriate or illegal activity has taken place. To add to any evidential trail for disciplinary action if necessary.

A Right to Privacy?

Everybody has a right to privacy, whether adult or child. But in certain circumstances there is a reduced expectation of privacy. In the context of this policy, that reduction is for security and safeguarding. This expectation is applicable whether it is school-owned equipment, or personally owned equipment used on the school network (and in some cases even if that personally owned equipment isn't used on the school network, but is used in school or for school business).

Managing Expectations

Consent is not a requirement for monitoring internet activities, however in complying with (General Data Protection Regulation 2018) Welling School clearly outlined in this policy that the internet may be subjected to monitoring (check your AUP).

WELLING SCHOOL

Part 8: Further information

UK Council for Internet Safety

The UK Council for Internet Safety (UKCIS) is a collaborative forum through which government, the tech community and the third sector work together to ensure the UK is the safest place in the world to be online – you can read it here:
https://www.gov.uk/government/organisations/uk-council-for-internet-safety

Teaching Online Safety in Schools

Guidance supporting schools to teach pupils how to stay safe online when studying new and existing subjects. https://www.gov.uk/government/publications/teaching-online- safety-in-schools

Relevant Legislations

Below is a list of legislations that should be considered when adhering to this E-safety policy.

- Education Act 1996
- Education and Inspections Act 2006
- Education Act 2011 Part 2 (Discipline)
- The School Behaviour (Determination and Publicising of Measures in Academies) Regulations 2012
- Health and Safety at Work etc. Act 1974
- Obscene Publications Act 1959
- Children Act 1989
- Human Rights Act 1998
- Computer Misuse Act 1990, amended by the Police and Justice Act 2006
- Defamation Act 1996
- Protection from Harassment Act 1997
- Freedom of Information Act 2000
- Regulation of Investigatory Powers Act (RIPA) 2000
- Safeguarding Vulnerable Groups Act 2006
- Equality Act 2010
- Common Law Duty of Confidentiality
- General Data Protection Regulation(GDPR) 2018

WELLING SCHOOL

Useful Websites

UK Council for Child Internet Safety (UKCCIS); http://www.education.gov.uk/ukccis/

Child Exploitation and Online Protection Centre (CEOP); http://ceop.police.uk/

UK Safer Internet Centre; http://www.saferinternet.org.uk

Childnet International; http://www.childnet.com/

SWGfL (South West Grid for Learning); http://www.swgfl.org.uk/

Cybermentors; https://cybermentors.org.uk/

Cyberbullying & the Law; https://www.anti-bullyingalliance.org.uk/tools-information/all-about-bullying/online-bullying/cyberbullying-and-law

Kidsmart: http://www.kidsmart.org.uk/

Child Safety Online:

https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/487973/ukccis_guide-final_____3_.pdf