Online Safety Policy

The Sittingbourne School

Approved by:	Lynn Lawrence	**Date:** November 2024
Last reviewed on:	November 2024	
Next review due by:	November 2025	

Contents

Introduction

Online safety is an essential part of safeguarding. The internet and technology-based devices are an essential part of everyday life and students should be empowered to build resilience and to develop strategies to manage and respond to risk online. The Sittingbourne School believes that online safety is an integral part of safeguarding and acknowledges its role to ensure that all students and staff are protected from any harm that may arise online.

The Designated Safeguarding Lead at The Sittingbourne School is Mrs O Wheeler.

1. Aims

The purpose of this policy is to:

- Have robust processes in place to ensure the online safety of pupils, staff, volunteers and governors
- Identify and support groups of pupils that are potentially at greater risk of harm online than others
- Deliver an effective approach to online safety, which empowers us to protect and educate the whole school community in its use of technology, including mobile and smart technology (which we refer to as 'mobile phones')
- Establish clear mechanisms to identify, intervene and escalate an incident, where appropriate

The 4 key categories of risk

Our approach to online safety is based on addressing the following categories of risk:

- **Content** – being exposed to illegal, inappropriate or harmful content, such as pornography, fake news, racism, misogyny, self-harm, suicide, antisemitism, radicalisation and extremism
- **Contact** – being subjected to harmful online interaction with other users, such as peer-to-peer pressure, commercial advertising and adults posing as children or young

adults with the intention to groom or exploit them for sexual, criminal, financial or other purposes

- **Conduct** – personal online behaviour that increases the likelihood of, or causes, harm, such as making, sending and receiving explicit images (e.g. consensual and non-consensual sharing of nudes and semi-nudes and/or pornography), sharing other explicit images and online bullying; and
- **Commerce** – risks such as online gambling, inappropriate advertising, phishing and/or financial scams

2. Legislation and guidance

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

- Teaching online safety in schools
- Preventing and tackling bullying and cyber-bullying: advice for headteachers and school staff
- Relationships and sex education
- Searching, screening and confiscation

It also refers to the DfE'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 pupils' electronic devices where they believe there is a 'good reason' to do so.

3. Roles and responsibilities

The Designated Safeguarding Lead has overall responsibility for online safety. However, all members of the school play an important role with regards to online safety. Acceptable use agreements are included in staff safeguarding training and the process for reporting concerns is the same as any other safeguarding issue. There is open dialogue between the IT manager and the Designated Safeguarding Lead to ensure that online safety has the prominence it requires. The acceptable use agreement is comprehensive and should be read alongside this protocol. The agreement includes: social media use; email expectations; use of personal devices and communication.

3.1 All governors will:

- Ensure they have read and understand this policy
- Agree and adhere to the terms on acceptable use of the school's ICT systems and the internet (appendix 1)
- Ensure that online safety is a running and interrelated theme while devising and implementing their whole-school or college approach to safeguarding and related policies and/or procedures
- Ensure that, where necessary, teaching about safeguarding, including online safety, is adapted for vulnerable children, victims of abuse and some pupils with special educational needs and/or disabilities (SEND). This is because of the importance of recognising that a 'one size fits all' approach may not be appropriate for all children in all situations, and a more personalised or contextualised approach may often be more

suitable.

The governor who oversees online safety is Lynn Lawrence.

3.2 The Headteacher:

The headteacher is responsible for ensuring that staff understand this policy, and that it is being implemented consistently throughout the school.

3.3 The Designated Safeguarding Lead (DSL) will:

Details of the school's designated safeguarding lead (DSL) are set out in our child protection and safeguarding policy, as well as relevant job descriptions.

The DSL takes lead responsibility for online safety in school, in particular:

- 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 governing board to review this policy annually and ensure the procedures and implementation are updated and reviewed regularly
- Taking the lead on understanding the filtering and monitoring systems and processes in place on school devices and school networks
- Working with the ICT manager to make sure the appropriate systems and processes are in place
- Working with the headteacher, ICT manager and other staff, as necessary, to address any online safety issues or incidents
- Managing all online safety issues and incidents in line with the school's child protection policy
- Ensuring that any online safety incidents are logged and dealt with appropriately in line with this policy. Online safety incident are identified through Lightspeed software which is then logged onto the Safeguarding chronology for the specific student.
- Ensuring that any incidents of cyberbullying are logged and dealt with appropriately in line with the school behaviour policy
- 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
- Undertaking annual risk assessments that consider and reflect the risks children face
- Providing regular safeguarding and child protection updates, including online safety, to all staff, at least annually, in order to continue to provide them with relevant skills and knowledge to safeguard effectively

This list is not intended to be exhaustive.

3.4 Leadership and management team will:

- Ensure that online safety is viewed as a safeguarding issue and that practice is in line with national and local recommendations and requirements.
- Ensure there are appropriate and up-to-date policies regarding online safety;

including a staff code of conduct/behaviour policy and acceptable use policy, which cover acceptable use of technology.
- Ensure that online safety is embedded within a progressive curriculum, which enables all learners to develop an age-appropriate understanding of online safety.
- Support the DSL and any deputies by ensuring they have appropriate time and resources to fulfil their online safety responsibilities.
- Ensure there are robust reporting channels for the community to access regarding online safety concerns, including internal, local and national support.

3.5 It is the responsibility of all members of staff to:

- Read and adhere to the online safety protocol and acceptable use protocols.
- Take responsibility for the security of school systems and the data they use, or have access to.
- Model good practice when using technology and maintain a professional level of conduct in their personal use of technology, both on and off site.
- Staff personal mobile phones should not be used whilst involved in professional duties such as teaching or on duty.
- Embed online safety education in curriculum delivery, wherever possible.
- Have an awareness of a range of online safety issues and how they may be experienced by the children in their care.
- Identify online safety concerns and take appropriate action by following the school's safeguarding policies and procedures.
- Know when and how to escalate online safety issues, including signposting to appropriate support internally and externally.
- Take personal responsibility for professional development in this area.
- To support students to read and understand the student's acceptable use statement in a way which suits their age and ability.

3.6 The IT Team/Manager

- Provide technical support and perspective to the DSL and leadership team, especially in the development and implementation of appropriate online safety and procedures.
- Implement appropriate security measures (including password policies and encryption) to ensure that the school's IT infrastructure/system is secure and not open to misuse or malicious attack, whilst allowing learning opportunities to be maximised.
- Ensure that the schools filtering policy is applied and updated on a regular basis; responsibility for its implementation is shared with the leadership team.
- Report any filtering breaches to the DSL and leadership team, as well as, the school's Internet Service Provider or other services, as appropriate.
- Ensure that any safeguarding concerns, identified through monitoring or filtering breaches are reported to the DSL, in accordance with the school's safeguarding procedures.

3.7 It is the responsibility of students to:

- Engage in age appropriate online safety education opportunities.
- Read and adhere to the school acceptable use statement.
- Education and engagement with students
- The school will establish and embed a progressive online safety curriculum throughout the whole school, to raise awareness and promote safe and responsible internet use amongst students by:
    - Ensuring education regarding safe and responsible use precedes internet access.
    - Including online safety in relevant programmes of study.
    - Reinforcing online safety messages whenever technology or the internet is in use.
    - Educating students in the effective use of the internet to research; including the skills of knowledge location, retrieval and evaluation.
    - Teaching students to be critically aware of the materials they read and shown how to validate information before accepting its accuracy.
    - Training and engagement with staff

3.8 It is the responsibility of parents and carers to:

- Read the acceptable use procedure and encourage their children to adhere to them.
- Role model safe online behaviour.
- Seek support and guidance from the setting or other agencies if there are risks or concerns online about their child/children.
- Be aware of changes in behaviour which could indicate that their child is at risk of harm online.
- Abide by the acceptable use agreement.
- Support the school's approach to online safety and encourage and support safe online behaviour

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
- Parent resource sheet – Childnet

3.9 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 (appendix 1).

4. Education pupils about online safety

Pupils will be taught about online safety as part of the curriculum. All schools have to teach:

- Relationships and sex education and health education in secondary schools

In KS3, pupils 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

Pupils in KS4 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, pupils 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 that 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 that 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
- How people can actively communicate and recognise consent from others, including sexual consent, and how and when consent can be withdrawn (in all contexts, including online)
- Including online safety in Character Education and Sex Education (RSE) and computing programmes of study.
- Ensuring Personal Development Time provides ample opportunity for students to discuss Online Safety and develop an awareness of societal trends, issues and concerns

The safe use of social media and the internet will also be covered in other subjects where relevant. Where necessary, teaching about safeguarding, including online safety, will be adapted for vulnerable children, victims of abuse and some pupils with SEND.

Vulnerable learners

The Sittingbourne School recognises that some learners are more vulnerable online due to a range of factors. This may include, but is not limited to children in care, children with Special Educational Needs and Disabilities (SEND) or mental health needs, children with English as an additional language (EAL) and children experiencing trauma or loss.

The Sittingbourne School will ensure that differentiated and ability appropriate online safety education, access and support is provided to vulnerable learners: Targeted intervention groups responding to smoothwall, outcomes differentiated in lessons.
When implementing an appropriate online safety policy and curriculum The Sittingbourne School will seek input from specialist staff as appropriate, including the SENCO, Child in Care Designated Teacher.

5. Educating parents/carers about online safety

The school will raise parents/carers' awareness of internet safety in letters/emails/newsletter or other communications home, and in information via our website or social media accounts. This policy will also be shared with parents/carers via the website.

The school will let parents/carers know:

- What systems the school uses to filter and monitor online use (Lightspeed)
- What their children are being asked to do online, including the sites they will be asked to access and who from the school (if anyone) their child will be interacting with online (upon request)

If parents/carers have any queries or concerns in relation to online safety, these should be raised in the first instance with on the Pastoral Enquiry Form.

6. Training and engagement with staff

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, bulletins, online CPD and staff meetings).

By way of this training, all staff will be made aware that:

- Technology is a significant component in many safeguarding and wellbeing issues, and that children are at risk of online abuse
- Children can abuse their peers online through:
    - Abusive, threatening, harassing and misogynistic messages
    - Non-consensual sharing of indecent nude and semi-nude images and/or videos, especially around chat groups
    - Sharing of abusive images and pornography, to those who don't want to receive such content
- Physical abuse, sexual violence and initiation/hazing type violence can all contain an online element

Training will also help staff:

- Develop better awareness to assist in spotting the signs and symptoms of online abuse
- Develop the ability to ensure pupils can recognise dangers and risks in online activity and can weigh up the risks
- Develop the ability to influence pupils to make the healthiest long-term choices and

keep them safe from harm in the short term

The DSL and Deputies 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.

7. Cyberbullying

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 1 person or group by another person or group, where the relationship involves an imbalance of power. (See also the school behaviour policy.)

7.1 Preventing and addressing cyber-bullying

To help prevent cyber-bullying, we will ensure that:

- Pupils understand what it is and what to do if they become aware of it happening to them or others. We will ensure that pupils 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 pupils, explaining the reasons why it occurs, the forms it may take and what the consequences can be. Personal Development Time will discuss cyber-bullying with their tutor groups.
- Teaching staff are also encouraged to find opportunities to use aspects of the curriculum to cover cyber-bullying. This includes personal, social, health and economic (PSHE) education, and other subjects where appropriate.
- All staff, governors and volunteers (where appropriate) receive training on cyber-bullying, its impact and ways to support pupils, as part of safeguarding training
- The school also sends information/leaflets on cyber-bullying to parents/carers so 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 pupils, the school will use all reasonable endeavours to ensure the incident is contained.
- The DSL will report the incident and provide the relevant material to the police as soon as is reasonably practicable, if they have reasonable grounds to suspect that possessing that material is illegal. They will also work with external services if it is deemed necessary to do so.

7.2 Examining electronic devices

The headteacher, and any member of staff authorised to do so, can carry out a search and confiscate any electronic device that they have reasonable grounds for suspecting:

- Poses a risk to staff or pupils, and/or
- Is identified in the school rules as a banned item for which a search can be carried

out, and/or
- Is evidence in relation to an offence

Before a search, if the authorised staff member is satisfied that they have reasonable grounds for suspecting any of the above, they will also:

- Make an assessment of how urgent the search is, and consider the risk to other pupils and staff. If the search is not urgent, they will seek advice from a member of the safeguarding or pastoral teams. Explain to the pupil why they are being searched, how the search will happen, and give them the opportunity to ask questions about it
- Seek the pupil's co-operation

Authorised staff members may examine, and in exceptional circumstances erase, any data or files on an electronic device that they have confiscated where they believe there is a 'good reason' to do so.

When deciding whether there is a 'good reason' to examine data or files on an electronic device, the staff member should reasonably suspect that the device has, or could be used to:

- Cause harm, and/or
- Undermine the safe environment of the school or disrupt teaching, and/or
- Commit an offence

If inappropriate material is found on the device, it is up to the DSL/Headteacher to decide on a suitable response. If there are images, data or files on the device that staff reasonably suspect are likely to put a person at risk, they will first consider the appropriate safeguarding response. This may include referrals to appropriate agencies for additional support.

When deciding if there is a good reason to erase data or files from a device, staff members will consider if the material may constitute evidence relating to a suspected offence. In these instances, they will not delete the material, and the device will be handed to the police as soon as reasonably practicable. If the material is not suspected to be evidence in relation to an offence, staff members may delete it if:

- They reasonably suspect that its continued existence is likely to cause harm to any person, and/or
- The pupil and/or the parent/carer refuses to delete the material themselves

If a staff member **suspects** a device **may** contain an indecent image of a child (also known as a nude or semi-nude image), they will:

- **Not** view the image
- Confiscate the device and report the incident to the DSL (or equivalent) immediately, who will decide what to do next. The DSL will make the decision in line with the DfE's latest guidance on screening, searching and confiscation and the UK Council for Internet Safety (UKCIS) guidance on sharing nudes and semi-nudes: advice for education settings working with children and young people

Any searching of pupils will be carried out in line with:

- The DfE's latest guidance on searching, screening and confiscation

- UKCIS guidance on sharing nudes and semi-nudes: advice for education settings working with children and young people
- Our behaviour policy

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

7.3 Artificial intelligence (AI)

Generative artificial intelligence (AI) tools are now widespread and easy to access. Staff, pupils and parents/carers may be familiar with generative chatbots such as ChatGPT and Google Bard.

The Sittingbourne School recognises that AI has many uses to help pupils learn, but may also have the potential to be used to bully others. For example, in the form of 'deepfakes', where AI is used to create images, audio or video hoaxes that look real. This includes deepfake pornography: pornographic content created using AI to include someone's likeness.

The Sittingbourne School will treat any use of AI to bully pupils in line with our behaviour policy.

8. Acceptable use of the internet in school

All pupils, parents/carers, staff, volunteers and governors are expected to sign an agreement regarding the acceptable use of the school's ICT systems and the internet (appendices 1 to 3). 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 pupils, staff, volunteers, governors and visitors (where relevant) to ensure they comply with the above and restrict access through filtering systems where appropriate.

More information is set out in the acceptable use agreements in appendices 1 to 3.

9. Pupils using mobile devices in school

Pupils may bring mobile devices into school, but are not permitted to use them during the school day.

Any breach of the acceptable use agreement by a pupil may trigger disciplinary action in line with the school behaviour policy, which may result in the confiscation of their device.

10. Staff using work devices outside school

All staff members will take appropriate steps to ensure their devices remain secure. This includes, but is not limited to:

- Keeping the device password-protected – strong passwords are at least 8 characters, with a combination of upper and lower-case letters, numbers and special characters

(e.g. asterisk or currency symbol)
- Ensuring their hard drive is encrypted – this means if the device is lost or stolen, no one can access the files stored on the hard drive by attaching it to a new device
- Making sure the device locks if left inactive for a period of time
- Not sharing the device among family or friends
- Windows Defender is built into the school operating system (inclusive of antivirus and spyware)
- Keeping operating systems up to date by always installing the latest updates

Staff members must not use the device in any way that would violate the school's terms of acceptable use, as set out in appendix 1.

Work devices must be used solely for work activities.

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

11. How the school will respond to issues of misuse

Where a pupil misuses the school's ICT systems or internet, we will follow the procedures set out in our policies on behaviour and ICT and internet acceptable use. 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 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 that involve illegal activity or content, or otherwise serious incidents, should be reported to the police.

12. Monitoring and review

This policy will be reviewed by the Designated Safeguarding Lead every year. It will also be updated if any changes to the information are made during the year.

Interest usage is closely monitored with any issues or concerns raised immediately by the filtering system to the Designated Safeguarding Lead and Safeguarding Officers immediately. To ensure they have oversight of online safety, the Headteacher will be informed of online safety concerns, as appropriate. The named governor for safeguarding will report on a regular basis to the governing body on online safety practice and incidents, including outcomes. Any issues identified via monitoring will be incorporated into our action planning.

13. Reducing risks online

The Sittingbourne School recognises that the internet is a constantly changing environment with new apps, devices, websites and material emerging at a rapid pace.
We will:

- Regularly review the methods used to identify, assess and minimise online risks.
- Examine emerging technologies for educational benefit and undertake appropriate risk assessments before use in the setting is permitted.

- Ensure that appropriate filtering and monitoring is in place and take all reasonable precautions to ensure that users can only access appropriate material.
- Due to the global and connected nature of the internet, it is not possible to guarantee that unsuitable material cannot be accessed via our computers or devices.
- All members of the community are made aware of our expectations regarding safe and appropriate behaviour online and the importance of not posting any content, comments, images or videos which could cause harm, distress or offence to members of the community.

12.Policy Links

- Acceptable use agreement for staff and for students.
- Child protection and safeguarding policy
- Behaviour policy
- Mobile phone policy
- Staff disciplinary procedures
- Data protection and privacy notices
- Complaints procedure

13.Useful Links for Educational Settings

Kent Support and Guidance:

- Swale Education Safeguarding Service
    - o Call: 03000 418 503
- If you are concerned about a child in Kent contact the Front Door on 03000 411111 or Frontdoor@kent.gov.uk
- Kent Safeguarding Children Multi-Agency Partnership 03000 421126 kscmp@kent.gov.uk
- **Kent Support and Guidance for Educational Settings**
    - https://www.kelsi.org.uk/child-protection-and-safeguarding
    - https://www.theeducationpeople.org/our-expertise/safeguarding/
- **Kent Police:**
    - www.kent.police.uk For non-urgent police contact 101 If you think the child is in immediate danger, you should call the police on 999.

National Links and Resources for Educational Settings

- CEOP:
    - o www.thinkuknow.co.uk
    - o www.ceop.police.uk
- Childnet: www.childnet.com
- Internet Matters: www.internetmatters.org
- Internet Watch Foundation (IWF): www.iwf.org.uk
- Lucy Faithfull Foundation: www.lucyfaithfull.org
- NSPCC: www.nspcc.org.uk/onlinesafety
    - o ChildLine: www.childline.org.uk

- o Net Aware: www.net-aware.org.uk
- The Marie Collins Foundation: www.mariecollinsfoundation.org.uk
- UK Safer Internet Centre: www.saferinternet.org.uk
  - o Professional Online Safety Helpline: www.saferinternet.org.uk/about/helpline
- 360 Safe Self-Review tool for schools: www.360safe.org.uk

National Links and Resources for Parents/Carers

- Action Fraud: www.actionfraud.police.uk
- CEOP:
  - o www.thinkuknow.co.uk
  - o www.ceop.police.uk
- Childnet: www.childnet.com
- Get Safe Online: www.getsafeonline.org
- Internet Matters: www.internetmatters.org
- Internet Watch Foundation (IWF): www.iwf.org.uk
- Lucy Faithfull Foundation: www.lucyfaithfull.org
- NSPCC: www.nspcc.org.uk/onlinesafety
  - o ChildLine: www.childline.org.uk
  - o Net Aware: www.net-aware.org.uk
- The Marie Collins Foundation: www.mariecollinsfoundation.org.uk
- UK Safer Internet Centre: www.saferinternet.org.uk
- Online Safety Toolkit: Online Safety - Czone (eastsussex.gov.uk

Appendix 1: acceptable use agreement (staff, governors, volunteers and visitors)

Designated Safeguarding Lead:	Online Safety Coordinator	Online Safety Technical Coordinator
Mrs Orla Wheeler	Mrs Orla Wheeler	Mr Matthew Thrower

As a professional organisation with responsibility for children's safeguarding it is important that all staff take all possible and necessary measures to protect data and information systems from infection, unauthorised access, damage, loss, abuse and theft. All members of staff have a responsibility to use the school's computer system in a professional, lawful, and ethical manner. To ensure that members of staff are fully aware of their professional responsibilities when using Information Communication Technology and the school systems, they are asked to read and sign this Acceptable Use Agreement.

This is not an exhaustive list and all members of staff are reminded that ICT use should be consistent with the Trust's ethos, other appropriate policies and the law.

General Online Safety

- I understand that information systems and ICT include networks, data and data storage, online and offline communication technologies and access devices. Examples include mobile phones, PDAs, digital cameras, email and social media sites.
- I have read and understood the school's online safety policy which covers the requirements for safe ICT use, including using appropriate devices, safe use of social media websites and the supervision of students within the classroom and other working spaces.
- I will report all incidents of concern regarding children's online safety to the Designated Safeguarding Lead or on Bromcom. I will report any accidental access, receipt of inappropriate materials, filtering breaches or unsuitable websites to Data Protection Officer on site.
- I will promote online safety with the students in my care and will help them to develop a responsible attitude to safety online, system use and to the content they access or create.
- I understand that my use of the information systems, the Internet and e-mail may be monitored and recorded to ensure policy/agreement compliance.
- If I have any queries or questions regarding safe and professional practice online either in school or off site, then I will raise them with the online safety coordinator.

Using ICT to Store Information

- I will not keep professional documents which contain school-related sensitive or personal information (including images, files, videos etc.) on any personal devices (such as laptops, digital cameras or mobile phones). Where possible I will use the Learning Platform to upload any work documents and files in a password protected environment. I will protect the devices in my care from unapproved access or theft.
- I will not store any personal information on the school computer system that is unrelated to school activities, such as personal photographs, music, video, files or financial information.

Communication

- My electronic communications with pupils/students, parents/carers and other professionals will only take place via work approved communication channels e.g. via a school provided email address or telephone number. Any pre-existing relationships which may compromise this will be discussed with the Designated Safeguarding Lead.
- E-mails and their content can be accessed by the Trust Principal/Head of School or their appointed representative if necessary

Security

- I understand that any hardware and software provided by my workplace for staff use can only be used by members of staff and only for educational use. To prevent unauthorised access to systems or personal data, I will not leave any information system unattended without first logging out or locking my login as appropriate. o Do not allow pupils to use your school laptop
    - Do not allow other staff to use your user account
- I will respect system security and I will not disclose any password or security information. I will use a 'strong' password. (A strong password has numbers, letters and symbols, has eight or more characters, does not contain a dictionary word and is only used on one system.)
    - Do not give out your password to other members of staff
- I will not attempt to install any purchased or downloaded software, including browser toolbars, or hardware without permission from the online safety Technical Coordinator.
- If I suspect a computer or system has been damaged or affected by a virus or other malware, or if I have lost any school related documents or files, then I will report this to the online safety Technical Coordinator as soon as possible.

Online Content

- I will not attempt to bypass any filtering and/or security systems put in place by the school. All access to the internet on the school site must be through the school network using school equipment.
- I will not create, transmit, display, publish or forward any material that is likely to harass, cause offence, inconvenience or needless anxiety to any other person, or any material which could bring my professional role, the school, Swale Academies Trust or the County Council, into disrepute.
- My use of ICT and information systems will always be compatible with my professional role, whether using school or personal systems. This includes the use of e-mail, text, social media, social networking, gaming, web publications and any

other devices or websites. My use of ICT will not interfere with my work duties and will be in accordance with the Trust's Acceptable Use Agreement and the law.

- Chat rooms, social networking sites, forums, communication, games, media streaming, auction, messaging, file sharing, online storage and sites that attempt to circumvent network and internet protection safeguards or unfairly dominate bandwidth are not allowed.
- Access to YouTube is permitted providing you adhere to the following:
    - Only search for a video during non-contact time and without children around (e.g. not in the computer suite if children are present).
    - Watch the video from the beginning to the end to ensure the content is entirely suitable.
    - Only view the video on the big screen so nothing else can be viewed at the side.
    - Do not, under any circumstances, search YouTube when children are present.
- Access to videos promoting extremism and radicalisation is permitted providing you adhere to the following:
    - Only search for a video during non-contact time and without children around (e.g. not in the computer suite if children are present).
    - Watch the video from the beginning to the end to ensure the content is entirely suitable.
    - Only view the video on the big screen so nothing else can be viewed at the side.
    - The video is used within the context of educational purposes.
    - The video is not used as a means to influence students into an extreme or radical view that may encourage discrimination of any individuals or groups of people.

Personal Devices

In the event that the school provides a wireless network for personal devices this is provided under the following conditions. The use of the school wireless for personal devices is provided under the following conditions. It is important to remember that the school is legally accountable for all personal data for which it is responsible, regardless of the ownership of the device.

Support

- The school accepts no responsibility for damage to personal devices caused by viruses, spyware, Trojans or other malware.
- Personal devices are brought into school at the users own risk. Please make sure you have adequate home insurance. Swale Academies Trust accepts no responsibility for damage or loss of personal devices.
- Personal devices are not part of the school's IT support remit, therefore no support can be provided for these devices.

User Access

- Personal devices connected to the school's network will only be used by the user account holder.
- Pupils/students must not be allowed to use personal devices owned by members of staff.
- If multiple devices per user are found connected to the school's network, they will be disabled.
- Access to the school's network for personal devices can be removed / disabled at any time.
- The Trust strongly recommends that you put in place procedures to prevent other users of the device accessing any school related content.
- Staff are provided with adequate school equipment. Do not rely on personal devices for lesson delivery.

Security

- Personal devices must have the capability to be remotely wiped and this must be enabled. The ActiveSync guide must be followed where applicable.
- A unique secure password must be set on the personal device and the user account to access the school's network.
- The wireless password for your specific device is for one user/device only.
- Use of personal devices is monitored when devices are connected to the school's network.
- Approximate location of devices can be tracked via the closest wireless access point when devices are connected to the school's network.
- Creating Wi-Fi hotspots via USB, wireless, Bluetooth, NFC or other communication methods is strictly prohibited.
- Loss of the device for any reason should be reported immediately to the online safety Technical Coordinator.
- Swale Academies Trust recommends that:
    - All content on personal devices should reflect the school's stance on professionalism
    - You put in place sufficient security measures to protect your personal content on any personal device.

Internet Access

- Internet access is based on 'staff' level of access.
- Some applications (Apps) might not work due to the nature of the filtering system.
- Applications (Apps) for personal email, storage and social networking are blocked on personal devices.*Data and E-mail Storage*
- Existing school policy regarding data storage and personal e-mail access applies to all personal devices.
- School related personal information (contact info, names, photos etc.) will not be stored on personal devices.
- When connected to the school's network, content on personal devices may be monitored.
- Devices with removable media maybe subject to data theft/loss separate from the device. Any theft or loss of removable media should be reported to the online safety Technical Coordinator.
- The device should be securely wiped when sold or transferred.

Legal Requirements

- School owned information systems must be used appropriately. I understand that the Computer Misuse Act 1990 makes the following criminal offenses: to gain unauthorised access to computer material; to gain unauthorised access to computer material with intent to commit or facilitate commission of further offenses or to modify computer material without authorisation.
- I will ensure that any personal data of pupils/students, staff or parents/carers is kept in accordance with the Data Protection Act 1988. This means that all personal data will be obtained and processed fairly and lawfully, only kept for specific purposes, held no longer than necessary and will be kept private and secure with appropriate security measures in place, whether used in the workplace, hosted online (only within countries or sites with suitable data protection controls) or accessed remotely. Any data which is being removed from the school site (such as via e-mail or on memory sticks or CDs) will be encrypted by a method approved by the Trust. Any images or videos of pupils/students will only be used as stated in the school image use policy and will always take into account parental consent.
- I will respect copyright and intellectual property rights.

The Trust may exercise its right to monitor the use of information systems, including Internet access and the interception of emails in order to monitor compliance with this Acceptable Use Agreement and the school's Data Security Policy. Where it believes unauthorised and/or inappropriate use of the service's information system or unacceptable or inappropriate behaviour may be taking place, the school will invoke its disciplinary procedure. If the school suspects that the system may be being used for inappropriate communication, criminal purposes or for storing unlawful text, imagery or sound, the matter will be brought to the attention of the relevant law enforcement organisation.

I have read and understood and agree to comply with the Swale Academies Trust Staff ICT Acceptable Use Agreement.

Full Name (BlockCapitals):_____

Staff Code (where applicable): _____

Date:_____

Signature_____

Please sign and return the complete form to the online safety Coordinator

Alternatively, please complete agreement on google classroom by marking as complete once you read and agree.

Please note:

- *Swale Academies Trust Staff ICT Acceptable Use Agreement remains the current Staff ICT Acceptable Use Agreement until such time as it is replaced.*
- *School refers to any primary school, secondary school or other establishment that is part of Swale Academies Trust.*

Designated Safeguarding Lead:	**Online Safety Coordinator**	**Online Safety Technical Coordinator**
Mrs Orla Wheeler	Mrs Orla Wheeler	Mr Matthew Thrower