Online Safety at Effingham Schools Trust

Schools	*Effingham Schools Trust: Cranmore and St Teresa's Schools*	
Author/Owner:	*Sarah Gallop* *Jessica Schembri* *Rachel Whitton* *Joe Matthews*	*DSL Cranmore Prep* *DSL Cranmore Senior* *DSL St Teresa's School* *Head of IT*
Heads:	*Claire McShane* *Barry Everitt*	*St Teresa's Prep School* *St Teresa's Senior School* *Cranmore*
Approved by (Board of Directors/Governing Body/Governors Sub Committee):	*Name:* Sally Hayes: St Teresa's Safeguarding Governor, Sue Walker: Cranmore Safeguarding Governor	*Signature:*
Date of Approval:	*November 2024*	
Monitoring and Revision due:	The online safety policy will be reviewed annually by the DSL team across the Trust It will also be reviewed to align with national, regional and local legislative or statutory changes. The next anticipated review date will be: September 2025 or earlier if new guidance is released.	

Policy Overview:
The purpose of this policy is to safeguard and protect all members of Effingham Schools Trust online community by providing a framework to promote and maintain a safe, effective and responsive online safety culture. The policy is applicable to all members of St Teresa's and Cranmore. This includes staff, students and pupils, volunteers, parents/carers, visitors and community users who have access to and are users of both St Teresa's digital technology systems and Cranmore's digital technology systems, both internally and externally.

References:

Department for Education (DfE) (2024) Keeping Children Safe in Education: statutory guidance for schools and colleges. London: DfE.

Department for Education (DfE) (2023) Teaching online safety in school: guidance supporting schools to teach their pupils how to stay safe online, within new and existing school subjects. London: DfE.

Department for Education (DfE) (2023) Working together to safeguard children. London: DfE.

Department for Education (2014) Cyberbullying: Advice for headteachers and school staff. London: DfE.

- Children Act 1989
- Children Act 2004
- Communications Act 2003
- Computer Misuse Act 1990
- Criminal Justice and Courts Act 2015
- Data Protection Act 2018
- Education Act 2011
- Education and Inspections Act 2006
- Freedom of Information Act 2000
- Malicious Communications Act 1988
- Serious Crime Act 2015
- Voyeurism (Offences) Act 2019
- Independent School Standards Regulations 2014 (ISSR) Part 3
- General Data Protection Regulation (GDPR) 2018
- Human Rights Act 1998
- Department for Education (DfE) (2024) Mobile phones in school
- Department for Education (DfE) (2023) 'Meeting Digital and Technology Standards in Schools and Colleges' (2024)

This Policy links with other Policies and Practices

- Whistleblowing
- Anti-bullying
- Acceptable Use Policy and Agreement (AUP)
- Behaviour Policy
- Safeguarding Child Protection Policy including use of images and mobile phones
- Staff Code of Conduct/ Staff Behaviour Policy
- Complaints Procedure
- Data Protection Policy
- Curriculum Policies

Disclaimer

Every effort has been made to ensure that the information contained within this policy is up to date and accurate and reflective of the latest legislative and statutory guidance. If errors are brought to our attention, we will correct them as soon as is practicable.

CRANMORE ST TERESA'S

CONTENTS

1. Introduction

Online safety in schools is of paramount importance. As the online world evolves, so do both the online harms and risks facing our children and the relevant legislation, both statutory and non-statutory, which directs and guides how schools should meet their online safety requirements.

School staff, members of the Effingham Schools Trust and governors play a vital role in setting an example for the schools and are central to implementing policy and process. It is imperative that a whole school community approach to online safety is adopted and that all stakeholders are aware of their responsibilities and duties in relation to keeping children safe online. This will support a robust online safety ethos and ensure that schools are providing the best online safety provision they possibly can and identify that where there are child welfare concerns, we will take action to address them.

This policy is applicable to all members of St Teresa's and Cranmore. This includes, staff, students and pupils, volunteers, parents/carers/guardians, visitors and community users who have access to and are users of either St Teresa's digital technology systems or Cranmore's digital Technology, both internally and externally within the home and community setting.

2. Online Safety School Statement

Effingham Schools Trust asserts that online safety is an essential element of safeguarding and duly acknowledges its statutory obligation to ensure that all learners and staff are protected from potential online harm.

We acknowledge that the internet and associated devices are an integral part of everyday life, and that all learners should be empowered to build resilience and to develop strategies to recognise and respond to online risks.

3. Policy Scope

Online safety is an omnipresent topic which requires recurrent regulatory review and places a stringent duty of care on us all. This policy supports the Effingham Schools Trust meeting statutory requirements as per the DfE guidance under 'Keeping children safe in Education' (2024), 'Working together to Safeguard Children' (2023) and the DfE document 'Meeting Digital and Technology Standards in Schools and Colleges' (2024). Effective, timely and robust online safety is fundamental to protecting children and young people in education and it is a significant part of the safeguarding agenda. The requirement to ensure that children and young people are able to use the internet and related communication technologies appropriately and safely, is a vital part of the wider duty of care to which all who work at Effingham Schools Trust are bound.

High quality online safety provision requires constant vigilance and a readiness to act where abuse, exploitation or neglect is suspected. The landscape of safeguarding is constantly evolving, and educational establishments must endeavour to embrace and shape their key priorities in support of this. Education has a vital role to fulfil in protecting children and young people from forms of online abuse whilst demonstrating a concerted obligation to respond with haste and flexibility to concerns as they arise. Above all, all staff must foster dedication to ensuring that they listen to the voices of the vulnerable and act upon what is heard. Safeguarding is everyone's responsibility.

Defining online abuse: "*Online abuse is any type of abuse that happens on the web, whether through social networks, playing online games or using mobile phones"* (NSPCC, 2019).

Hidden harms – types of online abuse may include:

- Cyberbullying
- Emotional abuse

- Grooming
- Sexting
- Sexual abuse
- Sexual exploitation

The types, patterns and different circumstances of significant harm and abuse should be considered within the categories identified for children in the Children Act 1989 / 2004. These are:

- Neglect
- Sexual
- Physical
- Emotional

Technology can facilitate a world of learning and development in addition to help yield a range of opportunities. However, the stark reality is that it can also present a window to potential and actual harm and abuse. It can elicit and support an array of illegal abusive behaviours including, but not limited to:

- harassment
- stalking
- threatening behaviour
- creating or sharing child sexual abuse material
- inciting a child to sexual activity
- sexual exploitation
- grooming
- sexual communication with a child
- causing a child to view images or watch videos of a sexual act.

Whilst the use of these exciting and innovative tools in school and at home has been shown to raise educational standards and promote student achievement, the use of these new technologies can put young people at risk within and outside the school. Some of the dangers they may face include (KCSIE 2023):

- **Content**: being exposed to illegal, inappropriate or harmful content, for example: pornography, fake news, racism, misogyny, self-harm, suicide, anti-Semitism, radicalisation and extremism.

- **Contact**: being subjected to harmful online interaction with other users; for example: 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**: online behaviour that increases the likelihood of, or causes, harm; for example, 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, phishing1 and or financial scams.

Many of these risks reflect situations in the off-line world and it is essential that this online safety policy is used in conjunction with other school policies such as the Behaviour and Safeguarding and Child Protection policies. As with all other risks, it is impossible to eliminate those risks completely. It is therefore essential, through good educational provision to build students' resilience to the risks to which they may be exposed, so that they have the confidence and skills to face and deal with these risks. Effingham Schools Trust must demonstrate that it has provided the necessary safeguards to help ensure that they have done everything that could reasonably be

expected of them to manage and reduce these risks. Underpinning the following online safety policy are the frameworks and Government legislation set out in 'Keeping children safe in Education' (2024), 'Working together to Safeguard Children' (2023) and the DfE document 'Meeting Digital and Technology Standards in Schools and Colleges' (2024).

This policy should be read alongside the relevant policies relating to safeguarding of children and in addition to the associated statutory legislation and guidance as stipulated on page 1-2 of this policy.

Process for Monitoring the impact of the Online Safety Policy
The Schools will monitor the impact of the policy using:

- Logs of reported incidents
- Filtering and monitoring logs
- Internal monitoring data for network activity
- Feedback from learners, parents/carers and staff

4. Roles and Responsibilities

The following section outlines the online safety roles and responsibilities of all stakeholders across the online community. The Education and Inspections Act 2006 empowers Headteachers, to such extent as is reasonable, to regulate the behaviour of students when they are off the school site and empowers members of staff to impose disciplinary penalties for inappropriate behaviour. This is pertinent to incidents of cyber-bullying or other e-safety incidents covered by this policy, which may take place out of school, but is linked to membership of the school. This may include, for example, instances of where cyber bullying has taken place over the summer holidays and has continued into term time or if a pupil has brought the school into disrepute over social media using a personal device, or from their home. The school will deal with such incidents within this policy and associated behaviour, child-on-child abuse and sexual harassment policies and will, where known, inform parents of incidents of inappropriate online safety behaviour that take place out of school.

4.1 Teachers and Staff

All members of staff (teaching and non-teaching) have a responsibility to protect children online. This includes every member of staff who works at the school; heads, teachers, supply teachers, work-experience staff, office staff, nurses, caretakers, cleaners to name a few. All teachers and staff must always act in accordance with their own professional boundaries, upholding professional behaviour and conduct at all times.

All school staff need to:

- Be aware of and adhere to all policies in school which support online safety and safeguarding.
- Contribute to policy development and review.
- Support in the ownership and responsibility for the security of systems and the data accessed.
- Model good practice when using technology.
- Ensure that communication with students (email / Virtual Learning Environment (VLE) / voice) is on a professional level and only carried out using official school systems.
- Embed all online safety issues aspects of the curriculum and other school activities.
- monitor ICT activity in lessons, extracurricular and extended school activities
- Recognise that students using mobile phones may be using their own data access and not the school's Wi-Fi (not at Cranmore).
- Know the process for making referrals and reporting concerns.
- Know how to recognise, respond and report signs of online abuse and harm.
- Receive appropriate child protection training.

- Always act in the best interests of the child.
- Be responsible for their own continuing professional development in online safety.
- Have an understanding of the expectations, applicable roles and responsibilities in relation to filtering and monitoring.

4.2 Governors and Senior Leadership Teams

A governor's role for online safety in a school should include, but is not limited to:

- Upholding online safety as a safeguarding issue which is embedded across the whole school culture.
- Ensuring that their own knowledge and skill are refreshed at regular intervals to enable them to keep up-to-date with current research, legislation and trends.
- Understanding the unique risks associated with online safety and be confident that they have the relevant knowledge and up to date capability required to keep children safe whilst they are online
- Recognising the additional risks that children with SEN and disabilities (SEND) face online, for example, from online bullying, grooming and radicalisation and are confident they have the capability to support SEND children to stay safe online.
- Ensuring that children are provided with a safe environment in which to learn and develop.
- Ensuring that the school has appropriate filters and monitoring systems in place.
- Ensuring the school has effective policies and training in place.
- Carrying out risk assessments on effectiveness of filtering systems.
- Auditing and evaluating online safety practice.
- Ensuring there are robust reporting channels.
- Actively engaging with local and national events to promote positive online behaviour, e.g. Safer Internet Day and anti-bullying week.

4.3 Designated Safeguarding Lead (DSL) and Deputy Designated Safeguarding Lead (Deputy DSL)

Keeping Children Safe in Education states that:

"The designated safeguarding lead should take lead responsibility for safeguarding and child protection (including online safety and understanding the filtering and monitoring systems and processes in place). This should be explicit in the role holder's job description."

They (the DSL) "are able to understand the unique risks associated with online safety and be confident that they have the relevant knowledge and up to date capability required to keep children safe whilst they are online at School or college"

They (the DSL) "can recognise the additional risks that children with special educational needs and disabilities (SEND) face online, for example, from bullying, grooming and radicalisation and are confident they have the capability to support children with SEND to stay safe online"

While the responsibility for online safety is held by the DSL and cannot be delegated, the School may choose to appoint an Online Safety Lead or other relevant persons to work in support of the DSL in carrying out these responsibilities.

With respect to online safety, it is the responsibility of the DSL to:

- Ensure children and young people are being appropriately taught about and know how to use the internet responsibly.
- Ensure teachers and parents are aware of measures to keep children safe online through relevant training provision.
- Take responsibility for all safeguarding matters, including online safety.

- Collaborate with the Senior Leadership Team, the IT Managers and Computing Leads.
- Facilitate effective record keeping and the reporting and monitoring of all online safety concerns.
- Promote online safety and the adoption of a whole school approach.
- Maintain own training and learning needs, ensuring they are up to date with all matters relating to online safety.

4.4 Effingham Schools Trust Head of IT

- Collaborate with the Senior Leadership Team, the online safety lead and computing lead.
- Promote online safety and the adoption of a whole school approach.
- Embed appropriate support for staff to use the internet safely with their pupils
- Carrying out risk assessments on effectiveness of filtering systems.
- Auditing and evaluating online safety practice.

IT Provider

The DfE Filtering and Monitoring Standards states: "Senior leaders should work closely with governors or proprietors, the designated safeguarding lead (DSL) and IT service providers in all aspects of filtering and monitoring. Your IT service provider may be a staff technician or an external service provider."

"Day to day management of filtering and monitoring systems requires the specialist knowledge of both safeguarding and IT staff to be effective. The DSL should work closely together with IT service providers to meet the needs of your setting. You may need to ask filtering or monitoring providers for system specific training and support."

"The IT service provider should have technical responsibility for:

- maintaining filtering and monitoring systems
- providing filtering and monitoring reports
- completing actions following concerns or checks to systems

The Trusts' service provider should work with the senior leadership team and DSL to:

- procure systems
- identify risk
- carry out reviews
- carry out checks

The Trusts carries out all the online safety measures that the School's obligations and responsibilities require. The Provider follows and implements School Online Safety Policy and procedures and is responsible for ensuring that;

- They are aware of and follow the School Online Safety Policy and IT Online Safety and Technical Security Policy to carry out their work effectively in line with School policy
- The School's technical infrastructure is secure and is not open to misuse or malicious attack . Servers, wireless systems and cabling must be securely located and physical access restricted and individual workstations are protected by up to date virus software
- The School meets (as a minimum) the required online safety technical requirements as identified by the DfE Meeting Digital and Technology Standards in Schools & Colleges and guidance from local authority / MAT or other relevant body
- There is clear, safe, and managed control of user access to networks and devices
- They keep up to date with online safety technical information to effectively carry out their online safety role and to inform and update others

- The use of technology is regularly and effectively monitored in order that any misuse/attempted misuse can be reported to the DSL
- The filtering policy is applied and updated on a regular basis and its implementation is not the sole responsibility of any single person
- Requests from staff for sites to be removed from the filtered list will be considered by a member of SLT.
- Monitoring systems are implemented and regularly updated as agreed in School policies
- Systems are in place to regularly monitor and record the activity of uses of the school ICT systems and users are made aware of this in the Acceptable Use Policy.
- Users will be made responsible for the security of their username and password, must not allow other users to access the systems using their log on details and must immediately report any suspicion or evidence that there has been a breach of security.

4.5 Children and Young People

With respect to online safety in your school, children need to:

- Know who the DSL is.
- Engage in age appropriate online safety education opportunities.
- Contribute to policy development and review.
- Read and adhere to online safety policies and acceptable use agreements (signed at the start of each academic year or when a new joiner starts).
- Respect the feelings of others, both off and online.
- Take responsibility for keeping themselves and others safe online.
- Where and how to find help with any online incidents or concerns.
- How, when and where to report concerns and when to seek help from a trusted adult.

The UKCCIS 'Education for a Connected World' framework aims to equip children and young people for digital life. Over the years at an Effingham School Trust school, a child will cover the following topics within the curriculum:

- Self-image and identity
- Online relationships
- Online reputation
- Online bullying
- Managing online information
- Health, wellbeing and lifestyle
- Privacy and security
- Copyright and ownership

4.6 Parents and Carers

Parents and carers need to understand the risks that children face online to protect them from online dangers. Parents need to:

- Read and adhere to all relevant policies.
- Be responsible when taking photos/using technology at school events.
- Know who the school DSL is.
- Know how to report online issues.
- Support online safety approaches and education provision.
- Be a role model for safe and appropriate behaviour.
- Identify changes in children's behaviour that could indicate they are at risk of online harm or abuse.
- Take responsibility for the filtering, monitoring and regulating of their own IT systems at home

5. Education and Training

Safeguarding activity across the United Kingdom (UK) continues to intensify in volume and intricacy with national influences relating to political uncertainty, a rise in poverty, an increase in the ageing population, sustained funding pressures and increased demand for child and adult services.

Furthermore, a commitment to ensuring the provision of an integrated and highly robust safeguarding service for all ages is essential.

Effective online safety provision and promotion of the welfare of children and young people relies upon constructive relationships that are conducive to robust multi-agency partnership working. This can only be effective when all staff are knowledgeable, confident and equipped with the skills to deal with processes and procedures when concerns arise relating to online abuse or harm.

Online safety has a high emphasis on a competent well-established workforce, up to date policies and procedures, robust governance arrangements and collaborative practices.

5.1 Learners

All schools within the Effingham Schools Trust will promote safe and responsible internet use:

- Education regarding safe and responsible use and access of the internet.
- Include online safety in Personal, Social, Health and Economic (PSHE) education, Relationships and Sex Education (RSE) and Information Computer Technology studies.
- Reinforce online safety messages as a continuum.

All schools within the Effingham Schools Trust will support learner's understanding based on age and ability:

- Display Acceptable Use posters in all rooms with internet access.
- Share age appropriate Codes of Conduct with pupils/students and ask them to sign them to say that they have understood them and agree to abide by them
- Inform all learners of monitoring and filtering in place.
- Implement peer education strategies.
- Provide continuous training and education as part of their transition across key stages.
- Use alternative, complementary support where needed.
- Seek learner voice.

5.2 Vulnerable Learners

Vulnerable children who need our help the most are not only missing out on opportunities to flourish online but are often experiencing the very worst that the online world can be. Over 2 million children in England are living in families with complex needs. Many children are living in families with domestic abuse, parental substance abuse and mental health problems.

Staff of the schools within the Effingham Schools trust recognises that some learners are more vulnerable due to a range of factors. Those children may be:

- Receiving statutory care or support.
- Known to have experienced specific personal harm.
- With a disability, ill-health or developmental difficulties.

- In households or families with characteristics or locations that indicate higher potential likelihood of current and future harm.
- Vulnerable or of concern by virtue of their identity or nationality.
- At risk in relation to activity or institutions outside the home.
- Caring for others.

Effingham Schools Trust will ensure the effective and safe provision of tailored online safety education. EST will obtain input and advice from specialist staff as deemed necessary.

5.3 Staff

Staff within Cranmore and St Teresa's will:

- Ensure provision of robust policies and practices as part of induction and ongoing training provision.
- Provide up to date online safety training at least annually or more in line with legislative and statutory changes and/or online safety incidents arising.
- Ensure training will include recognition of risks and responding to concerns.
- Inform of monitoring and filtering processes.
- Make staff aware that their online conduct outside of work can impact upon their professional role and responsibilities.
- Advise of appropriate resources.
- Ensure that all staff are aware of procedures to follow in recognising, responding and reporting online safety concerns.
- Check websites in advance of lessons to ensure that they are suitable.
- Be vigilant when pupils are allowed to freely search the internet, e.g. using approved search engines
- Monitor pupils' use by monitoring and engaging with the pupils throughout the lesson and to be aware that students may be using mobile data to access the internet. (Only at St Teresa's)
- Accept that from time to time, for good educational reasons, pupils may need to research topics (e.g. racism, drugs, discrimination) that would normally result in internet searches being blocked. In such a situation, staff can request that the IT Provider can temporarily remove those sites from the filtered list for the period of study. Any request to do so, should also be cleared by a member of SLT.
- Teach pupils in all lessons to be critically aware of the materials / content they access online and be guided to validate the accuracy of information, with particular focus on scamming and changes in cyber-crime.
- Teach all pupils to acknowledge the source of information used and to respect copyright when using material accessed on the internet.

5.4 Parents and carers

EST schools will:

- Recognise and cultivate the essential role parents and carers have in fostering safer online safety practices in children and young people.
- Ensure provision of resources, support and advice.
- Ensure provision and adherence to online safety policies and other policies of relevance.
- Advise of how and when to raise concerns.
- Provide details of all relevant contacts (for example, the DSL).

6. Cultivating a safe environment

The online world develops and changes at a great speed. New opportunities, challenges and risks are appearing all the time. This can make it difficult for schools to stay up to date with the latest devices, platforms, apps, trends and related threats.

It is important to focus on the underpinning knowledge and behaviours that can help pupils to navigate the online world safely and confidently regardless of the device, platform or app. This teaching could be:

- built into existing lessons across the curriculum
- covered within specific online safety lessons
- covered using school-wide approaches (Teaching online safety in schools 2023)

Children should be educated in an age-appropriate way around:

- How to evaluate what they see online
- How to recognise techniques for persuasion
- Their online behaviour
- How to identify online risks
- How and when to seek support

6.1 Evaluate: **How to evaluate what they see online**

This will enable pupils to make judgements about what they see online and not automatically assume that what they see is true, valid or acceptable.

Cranmore and St Teresa's will help pupils to consider questions including:

- Is this website/URL/email fake? How can I tell?
- What does this cookie do and what information am I sharing?
- Is this person who they say they are?
- Why does someone want me to see this?
- Why does someone want me to send this?
- Why would someone want me to believe this?

6.2 Recognise: How to recognise techniques used for persuasion

This will enable pupils to recognise the techniques that are often used to persuade or manipulate others. A strong grasp of knowledge across many areas makes people less vulnerable to these techniques and better equipped to recognise and respond appropriately to strongly biased intent or malicious activity.

EST schools will help pupils to recognise:

- Online content which tries to make people believe something false is true and/or mislead (misinformation and disinformation).
- Techniques that companies use to persuade people to buy something.
- Ways in which games and social media companies try to keep users online longer (persuasive/sticky design)
- Criminal activities such as grooming.

6.3 Online Behaviour

This will *enable pupils to* understand what acceptable and unacceptable online behaviour looks like. EST schools will teach pupils that the same standard of behaviour and honesty applies online and offline, including the importance of respect for others. EST Schools will also teach pupils to recognise unacceptable behaviour in others.

EST schools will help pupils to recognise acceptable and unacceptable behaviour by:

- Looking at why people behave differently online. For example, how anonymity (you do not know me) and invisibility (you cannot see me) affect what people do.
- Looking at how online emotions can be intensified resulting in mob mentality.
- Teaching techniques (relevant on and offline) to defuse or calm arguments (for example, a disagreement with friends) and disengage from unwanted contact or content online; and
- Considering unacceptable online behaviours often passed off as so-called social norms or just banter. For example, negative language that can be used, and in some cases is often expected, as part of online gaming and the acceptance of misogynistic, homophobic and racist language that would never be tolerated offline.

6.4 Identify: How to identity online risks

This will enable pupils to identify possible online risks and make informed decisions about how to act. The focus should be to help pupils assess a situation, think through the consequences of acting in different ways and decide on the best course of action.

EST schools will help pupils to identify and manage risk by:

- Discussing the ways in which someone may put themselves at risk online.
- Discussing risks posed by another person's online behaviour.
- Discussing when risk taking can be positive and negative.
- Discussing "online reputation" and the positive and negative aspects of an online digital footprint. This could include longer-term considerations; i.e. how past online behaviours could impact on their future when applying for a place at university or a job for example.
- Discussing the risks vs the benefits of sharing information online and how to make a judgement about when and how to share and who to share with.
- Asking questions such as what might happen if I post something online? Who will see it? Who might they send it to?

6.5 How and when to seek support

This will enable pupils to understand safe ways in which to seek support if they are concerned or upset by something they have seen online.

EST schools will help pupils by:

- Helping them to identify who trusted adults are.
- Looking at the different ways to access support from the school, police, the National Crime Agency's Click CEOP reporting service for children and 3rd party organisations, such as Childline and the Internet Watch Foundation. This links to wider school policies and processes around reporting of safeguarding and child protection incidents and concerns to school staff (see Keeping Children Safe in Education 2024).
- Helping them to understand that various platforms and apps will have ways in which inappropriate contact or content can be reported.

7. Responding to Online Safety Concerns

The safety of the child and young person is of paramount importance. Immediate action may be required to safeguard investigations and any other children and young people. Any concern that children and young people may be at risk of harm or abuse must immediately be reported.

Online safety is recognised as part of the safeguarding responsibilities – the DSL should take lead responsibility for online safety concerns which should be recorded and actioned. Children and young people will be enabled (at a level appropriate to their age and ability) to share online concerns. The Child Protection Safeguarding policy for includes procedures to follow regarding online safety concerns.

It is assumed that all members of the school community will be responsible users of ICT, who understand and follow this policy. However, there may be times when infringements of the policy could take place, through careless or irresponsible or, very rarely, through deliberate misuse. Any such incidents should be reported to the DSL. All staff are reminded that there is a clear school Whistleblowing policy.

Remember:

- Child welfare is of principal concern – the best interests of children take precedence.
- If there is any immediate danger, contact the police on 999.
- Staff need to notifiy a member of the pastoral team or the DSL team
- Use CEOP's or c-SPA process if it requires.
- Always adhere to local safeguarding procedures and report to the DSL and Head within *Safeguarding policies*

8. Digital Conduct

Use of digital and video images - Photographic, Video

The development of digital imaging technologies has created significant benefits to learning, allowing staff and students instant use of images that they have recorded themselves or downloaded from the internet. However, staff and students need to be aware of the risks associated with sharing images and with posting digital images on the internet. Those images may remain available on the internet forever and may cause harm or embarrassment to individuals in the short or longer term. Employers are likely to carry out internet searches for information about potential and existing employees. The school will inform and educate users about these risks and will implement policies to reduce the likelihood of the potential for harm:
When using digital images, staff should inform and educate students about the risks associated with the taking, use, sharing, publication and distribution of images. In particular they should recognise the risks attached to publishing their own images on the internet e.g. on social networking sites

Staff are allowed to take digital / video images to support educational aims, but must follow school policy (Child Protection and Safeguarding policy) concerning the sharing, distribution and publication of those images. Those images should be taken on school equipment, the personal equipment of staff should not be used for such purposes. If a member of staff wants to use their own equipment they need the permission of the Deputy Head (Pastoral) (St Teresa's) or the Head Master (Cranmore).

Care should be taken when taking digital / video images that students are appropriately dressed and are not participating in activities that might bring the individuals or the school into disrepute. If in doubt, the individual should ask the advice from a member of SLT.).
Students must not take, use, share, publish or distribute images of other pupils without their permission. It must be recognised by the students that these permissions can change depending on the relationship between particular groups of students.

Photographs published on the website, or elsewhere that include students will be selected carefully and will comply with good practice guidance on the use of such images. The School's Term and Conditions clarifies what is permissible and parents are required to opt out of the sharing of such images when signing the school contract. Any images which are published should be without the full name of the individual pupil (unless permission has been agreed by the pupil and their parent).

- Particular care should be taken in subjects such as Art, where it may be necessary for students to capture images using digital media of semi-naked models as part of their portfolio work. Advice should be sought from the DSL for safeguarding if there are any concerns. The Art department has its own code of conduct for artists and photographers (St Teresa's).

Data Protection

Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 2018 which states that personal data must be:

- Fairly and lawfully processed
- Processed for limited purposes
- Adequate, relevant and not excessive
- Accurate
- Kept no longer than is necessary
- Processed in accordance with the data subject's rights
- Secure
- Only transferred to others with adequate protection.
- Staff must ensure that they are fully conversant with the School Data Protection policy. In the context of e safety, they should particularly:
- Use personal data only on secure password protected computers and other devices, ensuring that they are properly "logged-off" at the end of any session in which they are using personal data.
- Transfer data using encryption and secure password protected devices. When personal data is stored on any portable computer system, USB stick or any other removable media:
- It is good practice to password protect the device
- The device must offer approved virus and malware checking software
- The data must be securely deleted from the device, once it has been transferred or its use is complete

Communications

A wide range of rapidly developing communications technologies has the potential to enhance learning. The following list shows how the school currently considers the benefit of using these technologies for education outweighs their risks / disadvantages:

Appropriate activities/Good practice

When using communication technologies the school considers the following as good practice:

- The official school email service may be regarded as safe and secure and is monitored. Staff and students should therefore use only the school email service to communicate with others when in school, or on school systems (e.g. by remote access).
- Users need to be aware that email communications may be monitored
- Users must immediately report the receipt of any email that makes them feel uncomfortable, is offensive, threatening or bullying in nature to the DSL. The recipient must not respond to any such email. If the recipient is a pupil, they should inform any member of staff although it is likely that they will speak to their HOY in the first instance. The email should be printed and saved before any further action is taken by the DSL
- Any digital communication between staff and students or parents must be professional in tone and content. These communications may only take place on official (monitored) school systems. Personal email addresses, text messaging or public chat / social networking programmes must not be used for these communications.
- Information on the school Facebook and Instagram site will be uploaded by the designated member of staff and content is monitored by the Director of Marketing and the DSL. They

are also subject to the disciplinary procedures of the School and the Facebook and Instagram privacy policies.

- Students should be taught about email safety issues, such as the risks attached to the use of personal details. They should also be taught strategies to deal with inappropriate emails and be reminded of the need to write emails clearly and correctly and not include any unsuitable or abusive material.
- Personal information should not be posted on the school website and only official email addresses should be used to identify members of staff.
- The School Safeguarding and Child Protection policy and Staff code of conduct details the school's policy on the staff use of mobile phones.

Unsuitable / inappropriate activities

The school believes that the activities referred to in the following section would be inappropriate in a school context and that all users of the school IT system should not engage in any of the following activities in school or outside school when using school equipment or systems.

- Child sexual abuse images as laid out in statutory law (https://www.cps.gov.uk/legal/p_to_r/prohibited_images_of_children/#an01)
- Promotion or conduct of illegal acts, e.g. under the child protection, obscenity, computer misuse and fraud legislation
- Adult material that potentially breaches the Obscene Publications Act in the UK
- Criminally racist material in the UK
- Pornography
- Promotion of any kind of discrimination, racial or religious hatred
- Threatening behaviour, including promotion of physical violence or mental harm
- Any other information which may be offensive to colleagues or breaches the integrity of the ethos of the school or brings the school into disrepute
- Using school systems to run a private business
- Use systems, applications, websites or other mechanisms that bypass the filtering or other safeguards employed by the school
- Uploading, downloading or transmitting commercial software or any copyrighted materials belonging to third parties, without the necessary licensing permissions
- Revealing or publicising confidential or proprietary information (e.g. financial / personal information, databases, computer / network access codes and passwords)
- Creating or propagating computer viruses or other harmful files
- Carrying out sustained or instantaneous high volume network traffic (downloading / uploading files) that causes network congestion and hinders others in their use of the internet
- Online gambling should not be used by any of the pupils in school or outside school when using school equipment or systems. It should be remembered that gambling is illegal under the age of 18

9. Monitoring and Compliance

Monitoring Requirements	Analysing incident logs Checking curriculum planning for online safety lessons Student, pupils, parents and carers feedback
Monitoring Method	Part of written report
Monitoring Prepared by	DSL for each school
Monitoring Presented to	DSL team to the EST Pastoral and Safeguarding Committee
Frequency of Reporting	Annual

9. Approval Process

This policy has been developed by the DSL Teams across the Trust, EST Head of IT, Director of Operations and members of SLT from each school.

10. Dissemination and Communication Process

The policy will be placed in the Staff handbook. Cranmore will place this policy on the Staff Shared folder and St Teresa's will place the document on firefly. The policy will be publicised through an induction and training update, policy update briefings for staff and notified to the Governors Board through Pastoral and Safeguarding Committee.

Rules will be posted in all network rooms.

Summary sent to the new pupils in the induction pack.

11. Development of the Policy

This policy will be reviewed within a 2 year period, or earlier in the light of any incidents or investigations, legislative changes or developments in best employment practice, to ensure its continuing relevance and effectiveness.

Appendices

1. **Equality impact assessment tool**
2. **Financial Risk assessment**
3. **Checklist for review of key document**
4. **Process flow chart *[*insert locally agreed process*]***

APPENDIX 1
Equality Impact Assessment Tool

		Yes/No	Comments
1.	Does the policy/guidance affect one group less or more favourably than another on the basis of:		
	• Race	No	
	• Ethnic origins (including gypsies & travellers)	No	
	• Nationality	No	
	• Gender	No	
	• Culture	No	
	• Religion or belief	No	
	• Sexual orientation including lesbian, gay & bisexual people	No	
	• Age	Yes	This policy has internet filtering by age groups which is what is required.
	• Disability – learning disabilities, physical disability, sensory impairment & mental health problems	No	
2.	Is there any evidence that some groups are affected differently?	Yes	This is acceptable as the requirement is each age and stage is treated differently due to developmental changes.
3.	If you have identified potential discrimination, are any exceptions valid, legal and/or justifiable?	No	
4.	Is the impact of the policy/guidance likely to be negative?	No	
5.	If so, can the impact be avoided?	N/A	
6.	What alternatives are there to achieving the policy/guidance without the impact?	N/A	
7.	Can we reduce the impact by taking different action?	N/A	

APPENDIX 2
Financial Risk Assessment

	Title of document:	Yes/No
1.	Does the implementation of this document require any additional capital resources?	Yes – long term investment required for monitoring at St Teresa's site. Completed in Summer '24. Cranmore requires urgent investment for the improvement of Wi-Fi access to improve coverage and security. Full monitoring and flagging of activity concerning pupil devices can only be achieved when all pupils are in receipt of a managed school device (pending Pupil Laptop Policy to be launched in 2025). Staff are able to login from home using personal computers to access school data/systems which presents both cyber security and data protection risks. A long-term transition to 1-1 staff laptops should be factored into future budgets.
2.	Does the implementation of this document require additional revenue?	No
3.	Does the implementation of this document require additional manpower?	No
4.	Does the implementation of this document release any manpower costs through a change in practice?	Yes – increasing the use of devices will cause an increase to the support that in needed within both schools. A larger number of pupils with school managed laptops will lead to more visits to IT Support, the current office provision at Cranmore is not suitable due to its location and size.
5.	Are there additional staff training costs associated with implementing this document which cannot be delivered through current training programmes or allocated training times for staff?	No – we already do annual training for online safety for all staff.

APPENDIX 3
Checklist for the Review and Approval of Key Document

	Title of document being reviewed:	Yes/No/ Unsure	Comments
1.	**Title**		
	Is the title clear and unambiguous?	Yes	
	Is it clear whether the document is a guideline, policy, protocol or standard?	Yes	
2.	**Rationale**		
	Are reasons for development of the document stated?	Yes	
3.	**Development Process**		
	Is the method described in brief?	Yes	
	Identify which people have been involved in the development including stakeholders/users.	DSL Team across the Trust	
	Name	**Job Title**	
	Sarah Gallop Jessica Schembri Rachel Whitton	*DSL Cranmore* *DSL Cranmore Senior* *DSL St Teresa's*	
		Yes/No/ Unsure	**Comments**
	Do you feel a reasonable attempt has been made to ensure relevant expertise has been used?	Yes	DSLs and Head of Operations.
4.	**Content**		
	Is the objective of the document clear?	Yes	
	Is the target population clear and unambiguous?	Yes	
	Are the intended outcomes described?	Yes	
	Are the statements clear and unambiguous?	Yes	
5.	**Evidence Base**		
	Is the type of evidence to support the document identified explicitly?	Yes	
	Are key references cited?	Yes	
	Are the references cited in full?	Yes	
	Are supporting documents referenced?	Yes	
6.	**Approval**		
	Does the document identify which group will approve it?	Yes	

	Title of document being reviewed:	Yes/No/ Unsure	Comments
7.	**Dissemination and Implementation**		
	Is there an outline/plan to identify how this will be done?	Yes	
	Does the plan include the necessary training/support to ensure compliance?	Yes	
8.	**Document Control**		
	Does the document identify where it will be held?	Yes	
	Have archiving arrangements for superseded documents been addressed?	Yes	
9.	**Process to Monitor Compliance and Effectiveness**		
	Are there measurable standards or KPIs to support the monitoring of compliance with and effectiveness of the document?	Yes	
	Is there a plan to review or audit compliance with the document?	Yes	
10.	**Review Date:**		
	Is the review date identified?	Yes	
	Is the frequency of review identified? If so, is it acceptable?	Yes	
11.	**Overall Responsibility for the Document**		
	Is it clear who will be responsible for co-ordinating the dissemination, implementation and review of the document?	Yes	

Individual Approval (this section to be completed by managerial/professional lead)			
If you are happy to approve this document, please sign and date it and forward to the chair of the committee/group where it will receive final approval.			
Name		Date	
Signature			
Committee Approval			
If the committee is happy to approve this document, please sign and date it and forward copies to the person with responsibility for disseminating and implementing the document and the person who is responsible for maintaining the organisation's database of approved documents.			
Name		Date	
Signature			