

# EFFINGHAM

CRANMORE • MANOR HOUSE • ST TERESA'S

## Online Safety at Effingham Schools Trust

<b>Schools</b>	<i>Effingham Schools Trust: Cranmore and St Teresa's Schools</i>	
<b>Author/Owner:</b>	<i>Toby Heaver Jessica Schembri Rachel Whitton Natalie Izzard Tracey Fantham Joe Matthews</i>	<i>DSL Cranmore Prep DSL Cranmore Senior DSL St Teresa's School DSL at Manor House DSL at Manor House Head of IT</i>
<b>Heads:</b>	<i>Barry Everitt  Stuart Field  Tracey Fantham</i>	<i>Cranmore  St Teresa's School  Manor House</i>
<b>Approved by (Board of Directors/Governing Body/Governors Sub Committee):</b>	<i>Name: Sue Walker Safeguarding Governor at Cranmore Sally Hayes Safeguarding Governor at St Teresa's Adrian Ross Safeguarding at Manor House</i>	<i>Signature:</i>
<b>Date of Approval:</b>		
<b>Monitoring and Revision due:</b>	<p>The online safety policy will be reviewed annually by the DSL team across the Trust</p> <p>It will also be reviewed to align with national, regional and local legislative or statutory changes.</p> <p>The next anticipated review date will be: September 2026 or earlier if new guidance is released.</p>	

### 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 The Effingham Schools Trust: St Teresa's, Effingham Sixth Form, Cranmore and Manor House. This includes staff, students and pupils, volunteers, parents/carers, visitors and community users who have access to and are users of the technology systems, both internally and externally.

## Contents

Statement of Intent .....	3
1. Legal Framework.....	4
2. Roles & Responsibilities .....	5
IT Support Staff .....	6
The Head of IT .....	6
3. Managing Online Safety .....	8
Handling Online Safety Concerns .....	8
4. Cyber Bullying.....	9
5. Child-on child sexual abuse and harassment .....	9
6. Grooming and exploitation.....	10
Child sexual exploitation (CSE) and child criminal exploitation (CCE) .....	10
Radicalisation .....	11
7. Mental Health.....	11
8. Online Hoaxes and harmful online challenges.....	11
9. Cyber Crime .....	12
10. Online safety training for staff.....	12
11. Online safety and the curriculum .....	13
12. Use of technology in the classroom .....	14
13. Use of smart technology .....	14
14. Educating Parents.....	15
15. Internet Access.....	15
16 Filtering and monitoring online activity .....	16
17. Network Security .....	17
18. Emails.....	17
19. Generative Artificial Intelligence (AI) .....	17
20. Social Networking .....	19
Use on behalf of the school .....	20
21. The school website.....	20
22. Use of Devices School-owned devices .....	20
Personal devices.....	20
23. Monitoring and Review.....	21
Appendix 1 .....	22
APPENDIX 2 - Acceptable Use Policy.....	25

## Statement of Intent

Effingham Schools Trust understands that using online services is an important aspect of raising educational standards, promoting pupil achievement, and enhancing teaching and learning. The use of online services is embedded throughout Trust schools; therefore, there are several controls in place to ensure the safety of pupils and staff.

The breadth of issues classified within online safety is considerable, but they can be categorised into four areas of risk:

- **Content:** Being exposed to illegal, inappropriate or harmful material, e.g. pornography, fake news, self-harm and suicide, and discriminatory or extremist views.
- **Contact:** Being subjected to harmful online interaction with other users, e.g. peer pressure, commercial advertising, and adults posing as children or young adults with the intention to groom or exploit children.
- **Conduct:** Personal online behaviour that increases the likelihood of, or causes, harm, e.g. sending and receiving explicit messages, and cyberbullying.
- **Commerce:** Risks such as online gambling, inappropriate advertising, phishing and/or financial scams.

The measures implemented to protect pupils and staff revolve around these areas of risk. This policy has been created with the aim of ensuring appropriate and safe use of the internet and other digital technology devices by all pupils, staff and visitors.

## 1. Legal Framework

This policy has due regard to all relevant legislation and guidance including, but not limited to, the following:

- Online Safety Act 2023
- Voyeurism (Offences) Act 2019
- The UK General Data Protection Regulation (UK GDPR) Data Protection Act 2018
- Children Act 1989
- Children Act 2004
- Communications Act 2003
- Computer Misuse Act 1990
- Criminal Justice and Courts Act 2015
- Education Act 2011
- Education and Inspections Act 2006
- Freedom of Information Act 2000
- Malicious Communications Act 1988
- Serious Crime Act 2015
- DfE (2025) 'Filtering and monitoring standards for schools and colleges'
- DfE (2021) 'Harmful online challenges and online hoaxes'
- DfE (2025) 'Keeping children safe in education 2025' (KCSIE)
- DfE (2023) 'Teaching online safety in school'
- DfE (2022) 'Searching, screening and confiscation'
- DfE (2025) 'Generative artificial intelligence in education'
- DfE (2023) 'Working Together to safeguard children'
- DfE (2014) Cyberbullying: Advice for headteachers and school staff.
- 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)
- DfE (2017) Preventing and tackling bullying and cyber-bullying: advice for headteachers and school staff
- DfE (2025) Relationships and sex education (RSE) and health education
- DfE (2023) Protecting Children from Radicalisation
- Department for Digital, Culture, Media and Sport and UK Council for Internet Safety (2024) 'Sharing nudes and semi-nudes: advice for education settings working with children and young people (updated March 2024)'
- UK Council for Child Internet Safety (2020) 'Education for a Connected World – 2020 edition' National Cyber Security Centre (2020) 'Small Business Guide: Cyber Security'

## 2. Roles & Responsibilities

The **governing board** is responsible for:

- Ensuring that this policy is effective and complies with relevant laws and statutory guidance.
- Ensuring the DSL's remit covers online safety.
- Reviewing this policy on an annual basis.
- Ensuring their own knowledge of online safety issues is up to date by undertaking training.
- Ensuring all staff undergo safeguarding and child protection training, including online safety, at induction and at regular intervals.
- Ensuring that there are appropriate filtering and monitoring systems in place
- Ensuring that the effectiveness of filtering and monitoring systems is reviewed at least annually in liaison with ICT staff and service providers.
- Ensuring that the SLT and other relevant staff have an awareness and understanding of the filtering and monitoring provisions in place, and manage them effectively and know how to escalate concerns when identified.
- Ensuring that all relevant school policies have an effective approach to planning for, and responding to, online challenges and hoaxes embedded within them.
- Ensuring compliance with the DfE's 'Meeting digital and technology standards in schools and colleges' filtering and monitoring standards.

The **headteacher** is responsible for:

- Ensuring that online safety is a running and interrelated theme throughout the school's policies and procedures, including in those related to the curriculum, teacher training and safeguarding.
- Supporting the DSL and the deputy DSLs by ensuring they have enough time and resources to carry out their responsibilities in relation to online safety.
- Ensuring staff receive regular, up-to-date and appropriate online safety training and information as part of their induction and safeguarding training.
- Ensuring online safety practices are audited and evaluated.
- Supporting staff to ensure that online safety is embedded throughout the curriculum so that all pupils can develop an appropriate understanding of online safety.
- Organising engagement with parents to keep them up to date with current online safety issues and how the school is keeping pupils safe.
- Communicate regularly with parents to reinforce the importance of children being safe online.
- Recruitment: as part of the shortlisting process, consider carrying out an online search as part of their due diligence on shortlisted candidates to help identify any incidents or issues that have happened, and are publicly available online which the school/ academy might want to explore with applicants at interview.
- Working with the DSL and governing board to update this policy on an annual basis.

The DSL is responsible for:

- Taking the lead responsibility for online safety in the school.
- Undertaking training so they understand the risks associated with online safety and can recognise additional risks that pupils with SEND face online.
- Liaising with relevant members of staff on online safety matters, e.g. the SENCO and ICT support staff.
- Ensuring online safety is recognised as part of the school's safeguarding responsibilities and that a coordinated approach is implemented.
- Ensuring safeguarding is considered in the school's approach to remote learning.
- Establishing a procedure for reporting online safety incidents and inappropriate internet use, both by pupils and staff, and ensuring all members of the school community understand this procedure.
- Understanding and taking responsibility of the filtering and monitoring processes in place at the school.
- Ensuring that all safeguarding training given to staff includes an understanding of the expectations, roles and responsibilities in relation to filtering and monitoring systems at the school.
- Maintaining records of reported online safety concerns as well as the actions taken in response to concerns.
- Monitoring online safety incidents to identify trends and any gaps in the school's provision, and using this data to update the school's procedures.
- Reporting to the governing board about online safety on a termly basis.
- Working with the headteacher and ICT support staff to conduct half-termly light-touch reviews of this policy.
- Working with the headteacher and governing board to update this policy on an annual basis.

IT support staff are responsible for:

- Promoting online safety and the adoption of a whole school approach.
- Embedding 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.
- Providing technical support in the development and implementation of the school's online safety policies and procedures.
- Implementing appropriate security measures as directed by the headteacher.
- Ensuring that the school's filtering and monitoring systems are updated as appropriate.
- Maintaining filtering and monitoring systems.
- Providing filtering and monitoring reports.
- Completing actions following concerns or checks to systems.

The Head of IT:

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 Trust carries out all the online safety measures that the School's obligations and responsibilities require. The Provider follows and implements this policy and its 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 users 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.

All [staff](#) members are responsible for:

- Taking responsibility for the security of ICT systems and electronic data they use or have access to.
- Modelling good online behaviours.
- Maintaining a professional level of conduct in their personal use of technology.
- Having an awareness of online safety issues.
- Ensuring they are familiar with, and understand, the indicators that pupils may be unsafe online.
- Reporting concerns in line with the school's reporting procedure.
- Where relevant to their role, ensuring online safety is embedded in their teaching of the curriculum.

Pupils are responsible for:

- Adhering to the Acceptable Use Agreement and other relevant policies.
- Seeking help from school staff if they are concerned about something they or a peer have experienced online.
- Reporting online safety incidents and concerns in line with the procedures within this policy.

### 3. Managing Online Safety

All staff will be aware that technology is a significant component in many safeguarding and wellbeing issues affecting young people, particularly owing to the rise of social media and the increased prevalence of children using the internet.

The DSL has overall responsibility for the school's approach to online safety, with support from deputies and the headteacher where appropriate, and will ensure that there are strong processes in place to handle any concerns about pupils' safety online. The DSL should liaise with the police or children's social care services for support responding to harmful online sexual behaviour.

The importance of online safety is integrated across all school operations in the following ways:

- Staff and governors receive regular training
- Staff receive regular email updates regarding online safety information and any changes to online safety guidance or legislation
- Online safety is integrated into learning throughout the curriculum
- Assemblies are conducted regularly on the topic of remaining safe online

#### Handling Online Safety Concerns

Any disclosures made by pupils to staff members about online abuse, harassment or exploitation, whether they are the victim or disclosing on behalf of another child, will be handled in line with the Child Protection and Safeguarding Policy.

Staff will be aware that pupils may not feel ready or know how to tell someone about abuse they are experiencing, due to feeling embarrassed, humiliated, or threatened. Staff will be aware and recognise the importance of the presence and scale of online abuse or harassment, by considering that just because it is not being reported, does not mean it is not happening.

Staff will be aware that harmful online sexual behaviour can progress on a continuum, and appropriate and early intervention can prevent abusive behaviour in the future. Staff will also acknowledge that pupils displaying this type of behaviour are often victims of abuse themselves and should be suitably supported.

The victim of online harmful sexual behaviour may ask for no one to be told about the abuse. The DSL will consider whether sharing details of the abuse would put the victim in a more harmful position, or whether it is necessary in order to protect them from further harm. Ultimately the DSL will balance the victim's wishes against their duty to protect the victim and other young people. The DSL and other appropriate staff members will meet with the victim's parents to discuss the safeguarding measures that are being put in place to support their child and how the report will progress.

Confidentiality will not be promised, and information may be still shared lawfully, for example, if the DSL decides that there is a legal basis under UK GDPR such as the public task basis whereby it is in the public interest to share the information. If the decision is made to report abuse to children's social care or the police against the victim's wishes, this must be handled extremely carefully and appropriate support provided to the victim.



Concerns regarding a staff member's online behaviour are reported to the headteacher, who decides on the best course of action in line with the relevant policies, e.g. the Staff Code of Conduct, Child Protection and Safeguarding Policy, and Disciplinary Policy and Procedures. If the concern is about the headteacher, it is reported to the chair of governors.

Concerns regarding a pupil's online behaviour are reported to the DSL, who investigates concerns with relevant staff members, e.g. the headteacher and ICT support staff, and manages concerns in accordance with relevant policies depending on their nature, e.g. the Behaviour Policy and Child Protection and Safeguarding Policy.

Where there is a concern that illegal activity has taken place, the headteacher will contact the police.

The school will avoid unnecessarily criminalising pupils. The DSL will decide in which cases this response is appropriate and will manage such cases in line with the Child Protection and Safeguarding Policy.

All online safety incidents and the school's response are recorded by the DSL.

## 4. Cyber Bullying

Cyberbullying can include, but is not limited to, the following:

- Threatening, intimidating, discriminatory or upsetting messages
- Threatening or embarrassing media sent via electronic means
- Silent or abusive phone calls or using the victim's device to harass others, to make them think the victim is responsible
- Unpleasant or defamatory information/comments/messages posted online
- Abuse between young people in intimate relationships online

The school will be aware that certain pupils can be more at risk of abuse and/or bullying online, such as LGBTQ+ pupils and pupils with SEND.

Cyberbullying against pupils or staff is not tolerated under any circumstances. Incidents of cyberbullying are dealt with quickly and effectively wherever they occur in line with the Anti-bullying Policy.

## 5. Child-on child sexual abuse and harassment

All staff will be aware of the indicators of abuse, neglect and exploitation and understand where the risk of such harms can occur online. Staff will understand that this can occur both in and outside of school, off and online, and will remain aware that pupils are less likely to report concerning online sexual behaviours, particularly if they are using websites that they know adults will consider to be inappropriate for their age.

The following are examples of online harmful sexual behaviour of which staff will be expected to be aware:

- Threatening, facilitating or encouraging sexual violence
- Voyeurism and Upskirting
- Sexualised online bullying
- Unwanted and unsolicited sexual comments and messages
- Consensual or non-consensual sharing of sexualised imagery
- Abuse between young people in intimate relationships online

All staff will be aware of and promote a zero-tolerance approach to sexually harassing or abusive behaviour, and any attempts to pass such behaviour off as trivial or harmless. Staff will be aware that allowing such behaviour could lead to a school culture that normalises abuse and leads to pupils becoming less likely to report such conduct.

Staff will be aware that creating, possessing, and distributing indecent imagery of children, i.e. individuals under the age of 18, is a criminal offence, even where the imagery is created, possessed, and distributed with the permission of the child depicted, or by the child themselves.

The school will be aware that interactions between the victim of online harmful sexual behaviour and the alleged perpetrator(s) are likely to occur over social media following the initial report, as well as interactions with other pupils taking “sides”, often leading to repeat harassment. The school will respond to these incidents in line with the Child Protection and Safeguarding Policy.

The school responds to all concerns regarding online child-on-child sexual abuse and harassment. Concerns regarding online child-on-child abuse are reported to the DSL, who will investigate the matter in line with the Child Protection and Safeguarding Policy.

## 6. Grooming and exploitation

Grooming is defined as the situation whereby an adult builds a relationship, trust and emotional connection with a child with the intention of manipulating, exploiting and/or abusing them.

Staff will be aware that grooming often takes place online and that pupils who are being groomed are commonly unlikely to report this behaviour for many reasons.

Due to the fact pupils are less likely to report grooming than other online offences, it is particularly important that staff understand the indicators of this type of abuse. The DSL will ensure that online safety training covers online abuse, the importance of looking for signs of grooming, and what the signs of online grooming are, including but not limited to:

- Being secretive about how they are spending their time.
- Having an older boyfriend or girlfriend, usually one that does not attend the school and whom their close friends have not met.
- Having money or new possessions, that they cannot or will not explain.

### Child sexual exploitation (CSE) and child criminal exploitation (CCE)

Although CSE often involves physical sexual abuse or violence, online elements may be prevalent, e.g. sexual coercion and encouraging children to behave in sexually inappropriate

ways through the internet. In some cases, a pupil may be groomed online to become involved in a wider network of exploitation.

CCE is a form of exploitation in which children are forced or manipulated into committing crimes for the benefit of their abuser. While these crimes often take place in person, it is increasingly common for children to be groomed and manipulated into participating through the internet.

Where staff have any concerns about pupils with relation to CSE or CCE, they will bring these concerns to the DSL without delay, who will manage the situation in line with the Child Protection and Safeguarding Policy.

### Radicalisation

Radicalisation is the process by which a person comes to support terrorism and extremist ideologies associated with terrorist groups. This process can occur through direct recruitment, e.g. individuals in extremist groups identifying, targeting and contacting young people with the intention of involving them in terrorist activity, or by exposure to violent ideological propaganda. Children who are targets for radicalisation are likely to be groomed by extremists online to the extent that they believe the extremist has their best interests at heart, making them more likely to adopt the same radical ideology.

Staff members will be aware of the factors which can place certain pupils at increased vulnerability to radicalisation. Staff will be expected to exercise vigilance towards any pupils displaying indicators that they have been, or are being, radicalised.

Where staff have a concern about a pupil relating to radicalisation, they will report this to the DSL without delay.

## 7. Mental Health

The internet, particularly social media, can be the root cause of a number of mental health issues in pupils, e.g. low self-esteem and suicidal ideation.

Staff will be aware that online activity both in and outside of school can have a substantial impact on a pupil's mental state, both positively and negatively. The DSL will ensure that training is available to help ensure that staff members understand popular social media platforms and terminology, the ways in which social media and the internet in general can impact mental health, and the indicators that a pupil is suffering from challenges in their mental health. Concerns about the mental health of a pupil will be dealt with in line with the Mental Health Policy.

## 8. Online Hoaxes and harmful online challenges

For the purposes of this policy, an **“online hoax”** is defined as a deliberate lie designed to seem truthful, normally one that is intended to scaremonger or to distress individuals who come across it, spread on online social media platforms.

For the purposes of this policy, **“harmful online challenges”** refers to challenges that are targeted at young people and generally involve users recording themselves

participating in an online challenge, distributing the video through social media channels and daring others to do the same. Although many online challenges are harmless, an online challenge becomes harmful when it could potentially put the participant at risk of harm, either directly as a result of partaking in the challenge itself or indirectly as a result of the distribution of the video online – the latter will usually depend on the age of the pupil and the way in which they are depicted in the video.

Where staff suspect there may be a harmful online challenge or online hoax circulating amongst pupils in the school, they will report this to the DSL immediately.

The DSL will conduct a case-by-case assessment for any harmful online content brought to their attention, establishing the scale and nature of the possible risk to pupils.

The DSL and headteacher will only implement a school-wide approach to highlighting potential harms of a hoax or challenge when the risk of needlessly increasing pupils' exposure to the risk is considered and mitigated as far as possible.

## 9. Cyber Crime

Cyber-crime is criminal activity committed using computers and/or the internet. There are two key categories of cyber-crime:

- **Cyber-enabled** – these crimes can be carried out offline; however, are made easier and can be conducted at higher scales and speeds online, e.g. fraud, purchasing and selling of illegal drugs, and sexual abuse and exploitation.
- **Cyber-dependent** – these crimes can only be carried out online or by using a computer, e.g. making, supplying or obtaining malware, illegal hacking, and 'booting', which means overwhelming a network, computer or website with internet traffic to render it unavailable.

The school will factor into its approach to online safety the risk that pupils with a particular affinity or skill in technology may become involved, whether deliberately or inadvertently, in cyber-crime. Where there are any concerns about a pupil's use of technology and their intentions with regard to using their skill and affinity towards it, the DSL will consider a referral to the Cyber Choices programme, which aims to intervene where children are at risk of committing cyber-crime and divert them to a more positive use of their skills and interests.

The DSL and headteacher will ensure that pupils are taught, throughout the curriculum, how to use technology safely, responsibly and lawfully.

## 10. Online safety training for staff

The DSL will ensure that all safeguarding training given to staff includes elements of online safety, including how the internet can facilitate abuse and exploitation, and understanding the expectations, roles and responsibilities relating to filtering and monitoring systems. All staff will be made aware that pupils are at risk of abuse, by their peers and by adults, online as well as in person, and that, often, abuse will take place concurrently via online channels and in daily life.

Training will equip staff with the knowledge and confidence to identify signs of online harm, respond appropriately to disclosures or concerns, and support pupils in developing critical thinking skills and safe online behaviours.

Staff will also be guided on how to embed online safety themes across the wider curriculum, promoting a consistent, whole-school approach to digital safeguarding.

## 11. Online safety and the curriculum

The school references the DfE 'teaching online safety in schools' guidance during the creation of their curriculum. Online safety is embedded throughout the curriculum and teaching is always appropriate to pupils' ages and developmental stages. All Pupils will be taught about online safety as part of the curriculum in accordance with the government's guidance on relationships education, relationships and sex education (RSE) 2025. The outline of what will be covered at what Key Stage is found in Appendix I.

Pupils are taught the underpinning knowledge and behaviours that can help them to navigate the online world safely and confidently regardless of the device, platform or app they are using.

The underpinning knowledge and behaviours pupils learn through the curriculum include the following:

- How to evaluate what they see online
- How to recognise techniques used for persuasion
- Acceptable and unacceptable online behaviour
- How to identify online risks
- How and when to seek support
- Knowledge and behaviours that are covered in the government's online media literacy strategy

The online risks pupils may face online are always considered when developing the curriculum. The school's approach to teaching online safety in the curriculum will reflect the ever-evolving nature of online risks, ensuring pupils develop the knowledge and resilience to navigate digital spaces safely and responsibly. Online safety education will address four key categories of risk: content, contact, conduct, and commerce.

The DSL is involved with the development of the school's online safety curriculum. Pupils will be consulted on the online safety curriculum, where appropriate, due to their unique knowledge of the kinds of websites they and their peers frequent and the kinds of behaviours in which they engage online.

Relevant members of staff, e.g. the SENCO, and DSL will work together to ensure the curriculum is tailored so that pupils who may be more vulnerable to online harms, e.g. pupils with SEND and DSL, receive the information and support they need.

The school will also endeavour to take a more personalised or contextualised approach to teaching about online safety for more susceptible children, and in response to instances of harmful online behaviour from pupils.

Class teachers review external resources prior to using them for the online safety curriculum, to ensure they are appropriate for the cohort of pupils.

Before conducting a lesson or activity on online safety, the class teacher and DSL consider the topic that is being covered and the potential that pupils in the class have suffered or may be suffering from online abuse or harm in this way. The DSL advises the staff member on how to best support any pupil who may be especially impacted by a lesson or activity. Lessons and activities are planned carefully so they do not draw attention to a pupil who is being or has been abused or harmed online, to avoid publicising the abuse.

During an online safety lesson or activity, the class teacher will ensure a safe environment is maintained in which pupils feel comfortable to say what they feel and ask questions, and are not worried about getting into trouble or being judged.

If a staff member is concerned about anything pupils raise during online safety lessons and activities, they will make a report in line with the Child Protection and Safeguarding Policy.

If a pupil makes a disclosure to a member of staff regarding online abuse following a lesson or activity, the staff member will follow the reporting procedure outlined in the Child Protection and Safeguarding Policy.

## 12. Use of technology in the classroom

A wide range of technology is used during lessons, including the following:

- Laptop/Desktop Computers
- Mobile/Tablet Devices
- Internet and Email
- Photo/Video/Audio equipment

Prior to using any websites, tools, apps or other online platforms in the classroom, or recommending that pupils use these platforms at home, the class teacher always review and evaluates the resource. Class teachers ensure that any internet-derived materials are used in line with copyright law.

Pupils are supervised when using technology and/or online materials during lesson time – this supervision is suitable for their age and ability.

## 13. Use of smart technology

While the school recognises that the use of smart technology can have educational benefits, there are also a variety of associated risks which the school will ensure it manages.

Pupils will be educated on the acceptable and appropriate use of technology.

Pupils will not be permitted to use smart devices or any other personal technology whilst in the classroom without explicit permission and appropriate technological safeguards in place.

No Pupil bar those in the Effingham Sixth Form are permitted to use Mobile phones whilst on School site during the working school day.

Where there is a significant problem with the misuse of smart technology among pupils, the school will discipline those involved in line with the school's Behaviour Policy.

The school will hold assemblies, where appropriate, which address any specific concerns related to the misuse of smart technology and outline the importance of using smart technology in an appropriate manner.

The school will seek to ensure that it is kept up to date with the latest devices, platforms, apps, trends and related threats.

The school will consider the 4C's (content, contact, conduct and commerce) when educating pupils about the risks involved with the inappropriate use of smart technology and enforcing the appropriate disciplinary measures.

## 14. Educating Parents

The school will work in partnership with parents to ensure pupils stay safe online at school and at home. Parents are provided with information about the school's approach to online safety and their role in protecting their children.

Parents will be made aware of the various ways in which their children may be at risk online, including, but not limited to:

- Child sexual abuse, including grooming.
- Exposure to radicalising content.
- Sharing of indecent imagery of pupils, e.g. sexting.
- Cyberbullying.
- Exposure to age-inappropriate content, e.g. pornography.
- Exposure to harmful content, e.g. content that encourages self-destructive behaviour.

Parents will be informed of the ways in which they can prevent their child from accessing harmful content at home, e.g. by implementing parental controls to block age-inappropriate content.

Parental awareness regarding how they can support their children to be safe online is raised by the school via methods such as

- Letters and newsletters
- School website and links to external online resources, e.g. Child Exploitation and Online Protection Command (CEOP)
- High profile events, such as Safer Internet Day and Effingham School Trust Internet Safety Week
- Parent Webinars
- Information evenings

## 15. Internet Access

Pupils, staff and other members of the school community are only granted access to the school's internet network once they have read and agreed to an Acceptable Use Agreement

All members of the school community are encouraged to use the school's network, instead of mobile networks, as the network has appropriate filtering and monitoring to ensure individuals are using the internet appropriately for their age group. Use of VPNs to bi-pass these systems is recognised as a breach of the Acceptable Use Policy.

## 16. Filtering and monitoring online activity

The governing board will ensure the school has appropriate filters and monitoring systems in place and that it is meeting the DfE's 'Filtering and monitoring standards for schools and colleges'. The governing board will ensure 'over blocking' does not lead to unreasonable restrictions as to what pupils can be taught with regards to online teaching and safeguarding.

The DSL will ensure that specific roles and responsibilities are identified and assigned to manage filtering and monitoring systems and to ensure they meet the school's safeguarding needs.

Requests regarding making changes to the filtering system will be directed to the ICT support team. Prior to making any changes to the filtering system, ICT technicians and senior leaders will review the request. Any changes made to the system will be recorded by ICT support staff. Reports of inappropriate websites or materials will be made to an ICT technician immediately, who will investigate the matter and makes any necessary changes.

Deliberate breaches of the filtering system will be reported to the DSL and ICT support staff, who will escalate the matter appropriately. If a pupil has deliberately breached the filtering system, they will be disciplined in line with the Behaviour Policy. If a member of staff has deliberately breached the filtering system, they will be disciplined in line with the Disciplinary Policy and Procedure.

If material that is believed to be illegal is accessed, inadvertently or deliberately, this material will be reported to the appropriate agency immediately, e.g. the Internet Watch Foundation (IWF), CEOP and/or the police.

The school's network and school-managed devices will be appropriately monitored. All users of the network and school-managed devices will be informed about how and why they are monitored. Concerns identified through monitoring will be reported to the DSL who will manage the situation in line with the Child Protection and Safeguarding Policy.

All staff will receive regular training on the operation and purpose of filtering and monitoring systems, including their role in safeguarding.

Personal devices connected to the school's network will be subject to the same filtering and monitoring standards to ensure consistent safeguarding measures.

Filtering and monitoring systems will undergo at least an annual review to assess their effectiveness and relevance.



## 17. Network Security

A layered approach to security is taken at the school and is managed by ICT support staff. Antivirus security software is installed and kept up to date. Device firewalls are switched on at all times and application controls are employed to restrict access.

Staff and pupils will be advised not to download unapproved software or open unfamiliar email attachments and will be expected to report all malware and virus attacks to ICT support staff.

All members of staff have their own unique usernames and private passwords to access the school's systems. Pupils are provided with either their own unique username and private passwords or a shared account as appropriate. Staff members and pupils are responsible for keeping their passwords private. Passwords have a minimum and maximum length and require a mixture of letters, numbers and symbols to ensure they are as secure as possible.

Users inform ICT support staff if they forget their login details, who will arrange for the user to access the systems under different login details. Users are not permitted to share their login details with others and are not allowed to log in as another user at any time.

Users are required to lock access to devices and systems when they are not in use.

## 18. Emails

Staff and pupils are given approved school email accounts. Prior to being authorised to use the email system, staff and pupils must agree to the Acceptable Use Agreement. Personal email accounts are not permitted to be used for school. Any email that contains sensitive or personal information is only sent securely via encrypted email.

External emails directed to pupil accounts may be prevented/moderated depending on the age of the pupil.

Staff are not permitted to communicate with pupils or parents via personal email accounts.

Staff members and pupils are required report junk/phishing messages. The school's email system can be configured to reduce threats from emails and attachment.

Multi-Factor Authentication is enforced for all staff accounts and staff receive regular cyber security-awareness training.

Any cyber-incidents are managed in line with the Data and Cyber-security Breach Prevention and Management Plan.

## 19. Generative Artificial Intelligence (AI)

When deciding whether to use generative AI, safety will be the top priority. Any use of AI tools by staff and pupils will be carefully considered and assessed, evaluating the benefits and risks of its use in the school.

AI tools will only be used in situations where there are specified clear benefits that outweigh the risks, e.g. where it can reduce teacher workload, and the school will ensure that any use

of AI tools comply with wider statutory obligations, including those outlined in KCSIE.

Pupils will only be permitted to use generative AI in the school with appropriate safeguards in place, e.g. close supervision and the use of tools with appropriate filtering and monitoring features in place.

The school will take steps to prepare pupils for changing and emerging technologies, e.g. generative AI and how to use them safely and appropriately with consideration given to pupils' age.

For any use of AI, the school will:

- Comply with the Trust AI Policy
- Comply with age restrictions set by AI tools and open access large language models (LLMs).
- Consider online safety, including AI, when creating and implementing the school's approach to safeguarding and related policies and procedures.
- Consult KCSIE to ensure all statutory safeguarding obligations and AI tools are used safely and appropriately.
- Refer to the DfE's generative AI product safety expectations and filtering and monitoring standards.

The school will take steps to prepare pupils for changing and emerging technologies, e.g. generative AI and how to use them safely and appropriately with consideration given to pupils' age.

The school will ensure its IT system includes appropriate filtering and monitoring systems to limit pupil's ability to access or create harmful or inappropriate content through generative AI.

The school will ensure that pupils are not accessing or creating harmful or inappropriate content, including through generative AI.

The school will take steps to ensure that personal and sensitive data is not entered into generative AI tools and that it is not identifiable.

The school will make use of any guidance and support that enables it to have a safe, secure and reliable foundation in place before using more powerful technology such as generative AI.

## 20. Social Networking

Access to social networking sites is filtered as appropriate. Staff and pupils are not permitted to use social media for personal use during lesson time. Staff members are advised that their conduct on social media can have an impact on their role and reputation within the school. The Staff Code of Conduct contains information on the acceptable use of social media – staff members are required to follow these expectations at all times.

Staff are not permitted to communicate with pupils or parents over social networking sites in an official capacity and are reminded to alter their privacy settings to ensure pupils and parents are not able to contact them on social media.

Pupils are taught how to use social media safely and responsibly through the online safety curriculum.

Concerns regarding the online conduct of any member of the school community on social media are reported to the DSL and managed in accordance with the relevant policy.

### Use on behalf of the school

The school's official social media channels are only used for official educational or engagement purposes. Staff members must be authorised by the headteacher to access to the school's social media accounts.

All communication on official social media channels by staff on behalf of the school is clear, transparent and open to scrutiny.

## 21. The school website

The headteacher is responsible for the overall content of the school website – they will ensure the content is appropriate, accurate, up-to-date and meets government requirements.

The website complies with guidelines for publications including accessibility, data protection, respect for intellectual property rights, privacy policies and copyright law. Personal information relating to staff and pupils is not published on the website.

## 22. Use of Devices School-owned devices

Staff members may be issued with devices such as laptops, tablets, mobile phones etc to assist with their work.

Pupils are provided with school-owned devices as necessary to assist in the delivery of the curriculum.

School-owned devices are used in accordance with the acceptable use agreements.

ICT support staff monitor school-owned devices and automate the installation of software updates and antivirus definitions. No software, apps or other programmes can be downloaded onto a device without authorisation from ICT support staff.

Cases of staff members or pupils found to be misusing school-owned devices will be managed in line with the Disciplinary Policy and Procedure and Behavioural Policy respectively.

### Personal devices

Any personal electronic device that is brought into school is the responsibility of the owner/user.

Pupils must abide by the Pupil Device Policy, which requires personal laptops to be enrolled on the school's MDM (Mobile Device Management System) for applicable year groups.

Students are not permitted to use personal devices on site during school hours without explicit permission of the school.

Staff members are not permitted to use their personal devices during lesson time, other than in an emergency. Staff members are not permitted to use their personal devices to take photos or videos of pupils. Staff members are not permitted to store student/staff personal data on personal devices.

Staff members must report concerns about their colleagues' use of personal devices on the school premises in line with the Staff Code of Conduct and the Child Protection and Safeguarding Policy.

Where a pupil uses accessibility features on a personal device to help them access education, the arrangements and rules for conduct for this are developed and managed on a case-by-case basis.

Appropriate signage is displayed to inform visitors to the school of the expected use of personal devices. Any concerns about visitors' use of personal devices on the school premises are reported to the DSL.

## 23. Monitoring and Review

The governing board, headteacher and DSL review this policy in full on an annual basis and following any online safety incidents.

The next scheduled review date for this policy is September 2026

Any changes made to this policy are communicated to all members of the school community.

The Pupil Acceptable Use Agreement is to be read in conjunction with the Acceptable Use Policy, which is available at request.

## Appendix 1

All Pupils will be taught about online safety as part of the curriculum in accordance with the government's guidance on relationships education, relationships and sex education (RSE) 2025

In **Key Stage (KS) 1**, pupils will be taught to:

- Use technology safely and respectfully, keeping personal information private
- Identify where to go for help and support when they have concerns about content or contact on the internet or other online technologies

Pupils in **Key Stage (KS) 2** will be taught to:

- Use technology safely, respectfully and responsibly
- Recognise acceptable and unacceptable behaviour
- Identify a range of ways to report concerns about content and contact
- Be discerning in evaluating digital content

By the **end of primary school**, pupils will know:

- That people should be respectful in online interactions, and that the same principles apply to online relationships as to face-to-face relationships, including where people are anonymous. For example, the importance of avoiding putting pressure on others to share information and images online, and strategies for resisting peer pressure
- How to critically evaluate their online relationships and sources of information, including awareness of the risks associated with people they have never met. For example, that people sometimes behave differently online, including pretending to be someone else, or pretending to be a child, and that this can lead to dangerous situations. How to recognise harmful content or harmful contact, and how to report this
- That there is a minimum age for joining social media sites (currently 13), which protects children from inappropriate content or unsafe contact with older social media users, who may be strangers, including other children and adults
- The importance of exercising caution about sharing any information about themselves online. Understanding the importance of privacy and location settings to protect information online
- Online risks, including that any material provided online might be circulated, and that once a picture or words has been circulated there is no way of deleting it everywhere and no control over where it ends up
- That the internet contains a lot of content that can be inappropriate and upsetting for children, and where to go for advice and support when they feel worried or concerned about something they have seen or engaged with online

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:

- Rights, responsibilities and opportunities online, including that the same expectations of behaviour apply in all contexts, including online
- Online risks, including the importance of being cautious about sharing personal information online and of using privacy and location settings appropriately to protect information online. Pupils should also understand the difference between public and private online spaces and related safety issues
- The characteristics of social media, including that some social media accounts are fake, and / or may post things which aren't real / have been created with AI. That social media users may say things in more extreme ways than they might in face-to-face situations, and that some users present highly exaggerated or idealised profiles of themselves online
- Not to provide material to others that they would not want to be distributed further and not to pass on personal material which is sent to them. Pupils should understand that any material provided online might be circulated, and that once this has happened there is no way of controlling where it ends up. Pupils should understand the serious risks of sending material to others, including the law concerning the sharing of images
- That keeping or forwarding indecent or sexual images of someone under 18 is a crime, even if the photo is of themselves or of someone who has consented, and even if the image was created by the child and/or using AI-generated imagery. Pupils should understand the potentially serious consequences of acquiring or generating indecent or sexual images of someone under 18, including the potential for criminal charges and severe penalties including imprisonment. Pupils should know how to seek support and should understand that they will not be in trouble for asking for help, either at school or with the police, if an image of themselves has been shared. Pupils should also understand that sharing indecent images of people over 18 without consent is a crime
- What to do and how to report when they are concerned about material that has been circulated, including personal information, images or videos, and how to manage issues online
- About the prevalence of deepfakes including videos and photos, how deepfakes can be used maliciously as well as for entertainment, the harms that can be caused by deepfakes and how to identify them
- That the internet contains inappropriate and upsetting content, some of which is illegal, including unacceptable content that encourages misogyny, violence or use of weapons. Pupils should be taught where to go for advice and support about something they have seen online. Pupils should understand that online content can present a distorted picture of the world and normalise or glamorise behaviours which are unhealthy and wrong
- That social media can lead to escalations in conflicts, how to avoid these escalations and where to go for help and advice
- How to identify when technology and social media is used as part of bullying, harassment, stalking, coercive and controlling behaviour, and other forms of abusive and/or illegal behaviour and how to seek support about concerns
- That pornography, and other online content, often presents a distorted picture of people and their sexual behaviours and can negatively affect how people behave towards sexual partners. This can affect pupils who see pornographic content accidentally as well as those who see it deliberately. Pornography can also portray misogynistic behaviours and attitudes which can negatively influence those who see it

- How information and data is generated, collected, shared and used online
- That websites may share personal data about their users, and information collected on their internet use, for commercial purposes (e.g. to enable targeted advertising)
- That criminals can operate online scams, for example using fake websites or emails to extort money or valuable personal information. This information can be used to the detriment of the person or wider society. About risks of sextortion, how to identify online scams relating to sex, and how to seek support if they have been scammed or involved in sextortion
- That AI chatbots are an example of how AI is rapidly developing, and that these can pose risks by creating fake intimacy or offering harmful advice. It is important to be able to critically think about new types of technology as they appear online and how they might pose a risk



## APPENDIX 2 - Acceptable Use Policy (St Teresa's, Effingham Sixth Form)

### **Pupil Acceptable Use Agreement**

To be read in conjunction with the School's Acceptable Use Policy

**These rules will keep everyone safe.**

1. On-site, IT systems will be used for schoolwork and homework as directed by a member of staff.
2. I will not upload inappropriate material to my workspace. I will only edit or delete my own files, and not view or change other people's files without their permission.
3. I will only use my devices for work purposes during the school day.
4. I recognise that my device may be confiscated if I am using it inappropriately.
5. Headphones are only to be used on site, during the school day with the permission of a teacher.
6. I will not install or use VPNs whilst at school.
7. I will adhere to the Artificial Intelligence Policy, recognising the plagiarism, copyright, illegal implications of inappropriate use.
8. I will not take photographs or videos of people without their permission.
9. I will not upload to social media photos of other people without their permission.
10. I will only take pictures or videos that are required for a task or activity as directed by a member of staff. All unnecessary images or videos will be deleted immediately and must not be uploaded to social media without permission.
11. I will not create, upload or share any photos of myself or others in a state of undress.
12. If I receive rude or an embarrassing image or text I will not forward it on to other people.
13. Any videos I take in my social time away from school must not identify the school in anyway. We advise that you consider your digital footprint before posting anything online.
14. I will not download or install any software on to the IT Systems.
15. I will keep my logins, IDs and passwords secret, and only use my own login when accessing the school computers.
16. I will use the internet responsibly and will not visit websites I know to be banned by the school. I am also aware that during lessons I will be directed to websites that are appropriate for my studies by staff.
17. If a message from my antivirus software alerts me of a virus, I will report to a teacher as soon as possible.
18. I will only email people I know, or those approved by my teachers.
19. The messages I send, or information I upload will always be polite and sensible.
20. When emailing staff, I will always be polite and use correct forms of address, with no emojis or slang. An acceptable email may follow this format:  

*Dear Mr Field,*  
*Please find attached my homework.*  
*Kind regards,*  
*Jane Bloggs*
21. I will not send bulk email messages either internally or externally. We advise you are very cautious with the reply all button. Always double check before you press send.
22. I will not open attachments, or download a file, unless I have permission or I know and trust the person that has sent them.

23. I am aware that all IT use is logged and monitored and that this includes a record of all internet searches.
24. I will not give my home address, phone number, send photographs or video, or give any personal information that could be used to identify me or my family or my friends, unless a trusted adult has given me permission.
25. I will never arrange to meet someone I have only ever previously met on the Internet or by email or in a chat room, unless I take a trusted adult with me.
26. If I see anything I am unhappy with or I receive a message I do not like, I will not respond to it but I will save it and talk to a teacher or trusted adult.
27. I am aware that some websites and social networks have age restrictions and I should respect this and not access unsuitable websites.
28. I am aware that online activity at all times should not upset or hurt other people and that I should not put myself at risk.
29. I am aware that my use of the Internet to interact with other students can be used in school disciplinary proceedings, or handed to the police if necessary, even if this occurs out of school times.
30. When participating in live online learning sessions via platforms such as Teams, I will behave appropriately and responsibly. I will ensure any chatroom contributions are appropriate. I will ensure both my video and speaker are switched off during live streaming, unless instructed otherwise by the teacher.
31. Where appropriate, it is the parent's responsibility to monitor what their child accesses on their device at home and ensure they do not access any illegal materials.
32. Users are responsible for keeping their device up to date through software, security and app updates. The device is virus protected and should not be capable of passing on infections to the network.
33. Electronic devices are brought into the school entirely at the risk of the owner and the decision to bring the device into the school lies with the user (and their parents/carers) as does the liability for any loss or damage resulting from the use of the device in school.
34. The school accepts no responsibility or liability in respect of lost, stolen or damaged devices while at school or on activities organised or undertaken by the school (the school recommends insurance is purchased to cover that device whilst out of the home).
35. The school accepts no responsibility for any malfunction of a device due to changes made to the device while on the school network or whilst resolving any connectivity issues.
36. The school is not responsible for the day-to-day maintenance or upkeep of the users' personal device such as the charging of any device, the installation of software updates or the resolution of hardware issues

I have read and understood these rules and I agree to follow them at all times.

Signed: \_\_\_\_\_ Date: \_\_\_\_\_

Name: \_\_\_\_\_ Form: \_\_\_\_\_