

EFFINGHAM

CRANMORE • MANOR HOUSE • ST TERESA'S

Online Safety at Effingham Schools Trust

Schools	<i>Cranmore, St Teresa's School, Manor House School, Effingham Sixth Form</i>	
Author/Owner:	<i>Toby Heaver Jessica Schembri Claire Pitchford Clare Green 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>
Heads:	<i>Barry Everitt Stuart Field Tracey Fantham</i>	<i>Cranmore St Teresa's School Manor House</i>
Approved by (Board of Directors/Governing Body/Governors Sub Committee):	<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>
Date of Approval: <i>Reviewed:</i>	<i>March 2026 September 2026</i>	
Monitoring and Revision due:	<i>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 2027 or earlier if new guidance is released.</i>	

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	10
6. Grooming and exploitation.....	11
Child sexual exploitation (CSE) and child criminal exploitation (CCE)	11
Radicalisation	11
7. Mental Health.....	12
8. Online Hoaxes and harmful online challenges.....	12
9. Cyber Crime	12
10. Online safety training for staff.....	13
11. Online safety and the curriculum	13
12. Use of technology in the classroom	15
13. Use of smart technology	15
14. Educating Parents.....	16
15. Internet Access.....	16
16. Filtering and monitoring online activity	17
17. Network Security	18
18. Emails	18
19. Generative Artificial Intelligence (AI)	18
20. Social Networking	19
Use on behalf of the Trust.....	20
21. The Trust website	20
22. Use of Devices School-owned devices	20
Personal devices.....	21
23. Monitoring and Review.....	21
Appendix 1 – Online Safety Education.....	22
Appendix 2 - Acceptable Use Policy (St Teresa's, Effingham Sixth Form)	25
Appendix 3 - Acceptable Use Policy (Cranmore, Senior).....	27

Appendix 4 - Acceptable Use Policy (Cranmore, Year 6)	29
Appendix 5 - Acceptable Use Policy (Cranmore, Reception to Year 5)	31
Appendix 6 – Online Safety Policy for Boarding	32

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
- National Minimum Standards for Boarding
- DfE (2025) 'Filtering and monitoring standards for schools and colleges'
- DfE (2021) 'Harmful online challenges and online hoaxes'
- DfE (2026) 'Keeping children safe in education 2026' (KCSIE)
- DfE (2023) 'Teaching online safety in school'
- DfE (2022) 'Searching, screening and confiscation'
- DfE (2025) 'Generative artificial intelligence in education'
- DfE (2026) 'Working Together to safeguard children'
- DfE (2026) 'Independent School Standards, Guidance for Independent Schools'
- DfE (2014) Cyberbullying: Advice for headteachers and school staff.
- Human Rights Act 1998
- Department for Education (DfE) (2026) Mobile phones in school
- Department for Education (DfE) (2022) 'Meeting Digital and Technology Standards in Schools and Colleges'
- 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 filtering and monitoring provision is formally reviewed at least annually, and sooner following a significant incident, system change or identified risk, in liaison with the DSL and Head of IT.
- 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 Trust'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.
- Keeping parents and carers appropriately informed about online safety risks and the measures the Trust takes to keep pupils safe.
- 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 Trust/ 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 Trust.
- 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 Trust's safeguarding responsibilities and that a coordinated approach is implemented.
- Ensuring safeguarding is considered in the Trust'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 Trust community understand this procedure.
- Understanding and taking responsibility of the filtering and monitoring processes in place at the Trust.
- 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 Trust.
- 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 Trust's provision, and using this data to update the Trust's procedures.
- Reporting to the governing board about online safety on a termly basis.
- Working with the headteacher and Head of IT to complete documented half-termly safeguarding checks of filtering and monitoring reports, alerts, incidents and actions. These checks are not a full policy review.
- 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 Trust's online safety policies and procedures.
- Implementing appropriate security measures as directed by the headteacher.
- Ensuring that filtering and monitoring systems address harmful content in text, image, audio, video and AI-generated formats, insofar as the systems are technically capable of doing so.
- Maintaining filtering and monitoring systems.
- Providing filtering and monitoring reports.
- Completing actions following concerns or checks to systems.

The Head of IT is responsible for:

Working with senior leaders, DSLs, IT support staff and external service providers to ensure that technical controls support the Trust's safeguarding requirements.

In particular, the Head of IT will:

- Advise on the procurement and configuration of filtering, monitoring and security systems.
- Identify and assess technical risks, including changes to systems, devices, networks and online services.
- Implement technical controls approved through the Trust's safeguarding and IT governance arrangements.
- Provide monitoring reports and material alerts to the relevant DSL promptly.
- Coordinate technical checks and remedial actions, retaining appropriate records.
- Support the DSL and senior leaders with the annual review of filtering and monitoring provision and with additional checks following incidents, significant system changes or identified risks.
- Ensure that responsibilities delegated to IT support staff or external service providers are documented, understood and monitored.

External service providers act under the direction of the Head of IT and the Trust's safeguarding and IT governance arrangements. They must comply with this policy, contractual requirements and associated procedures, but accountability for safeguarding decisions remains with the Trust.

- 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 Trust 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.
- Being alert to online spaces that may expose pupils to harmful content relating to gender questioning, gender-related distress or exploitation, and reporting any concerns in accordance with safeguarding procedures. Gender questioning is not, by itself, a safeguarding concern; staff should focus on any identifiable distress, abuse, exploitation or other risk of harm.
- Reporting concerns in line with the Trust'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 Trust'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 disclosure by a pupil about online abuse, harassment or exploitation, whether concerning them or another child, will be handled in accordance with the Child Protection and Safeguarding Policy. The policy uses neutral terms such as "the child who has reported the concern" and "the child alleged to have caused harm" until findings have been established.

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.

Concerns involving a pupil who is questioning their gender will be considered sensitively and individually through the Trust's normal safeguarding procedures. Staff will listen to the pupil, avoid assumptions, consider any associated distress, abuse, exploitation or other risk of harm, and seek advice from the DSL. Parents or carers will be involved where appropriate and safe to do so, and relevant clinical information will be considered where available.

Staff will recognise that harmful online sexual behaviour can occur on a continuum and that early, appropriate intervention may prevent further harm. A child alleged to have caused harm may also have unmet safeguarding or welfare needs and should receive appropriate support, without diminishing the needs and safety of the child who has reported the concern.

The child who has reported the concern may ask for no one else to be told. Staff must not promise confidentiality. The DSL will explain, in an age-appropriate way, what information may need to be shared, with whom and why. The child's wishes and safety will be considered, but information will be shared where necessary to protect them or others. Parents or carers will normally be involved where appropriate and safe to do so.

Safeguarding information will be shared in accordance with the Trust's safeguarding and data protection procedures. Decisions will be based on the circumstances of the case and will use an appropriate lawful basis. Information shared must be necessary, proportionate, relevant, adequate, accurate, timely and secure, and limited to those who need it to safeguard the child or others. The rationale for sharing, or not sharing, information will be recorded. Consent is not required where there is a lawful basis to share information for safeguarding purposes.

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 will be reported to the DSL. The DSL will establish sufficient facts to assess risk, preserve relevant evidence and decide whether internal action or referral is required, working with the headteacher, Head of IT and other relevant staff. The Trust will not conduct enquiries that could prejudice a police or children's social care investigation.

Where there is concern that a criminal offence may have occurred, the DSL and headteacher will assess the matter under the Trust's safeguarding procedures and seek advice or make a referral to the police, children's social care or another appropriate agency. Immediate risks to life or safety will be reported to the emergency services without delay.

The Trust 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 Trust'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 Trust 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 Trust 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 Trust will respond to these incidents in line with the Child Protection and Safeguarding Policy.

The Trust 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 Trust 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 Trust, 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 Trust 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 Trust 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 Trust'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 Trust'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 Trust 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 Trust recognises that the use of smart technology can have educational benefits, there are also a variety of associated risks which the Trust 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.

The school recognises that safeguarding concerns involving mobile phones may occur outside school hours and can continue to impact pupils whilst in school. Such concerns will be managed through safeguarding and behaviour procedures where appropriate

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

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

The Trust 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 Trust will work in partnership with parents to ensure pupils stay safe online at school and at home. Parents are provided with information about the Trust'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 Trust 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 Trust community are only granted access to the Trust's internet network once they have read and agreed to an Acceptable Use Agreement

All members of the Trust community are encouraged to use the Trust'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 Trust 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 regard 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 Trust's safeguarding needs.

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

Deliberate breaches of the filtering system will be reported to the DSL and IT 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 Trust'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 Trust'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 Trust 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 Trust'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 Trust'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 considering the use of generative AI, the Trust will place safety, safeguarding and data protection at the forefront of all decision-making. Staff and pupils may only use AI tools where the benefits have been carefully assessed and are judged to outweigh any associated risks.

AI tools will only be used where there is a clear educational or operational benefit, such

as reducing administrative workload or improving efficiency. Any use of AI must comply with all relevant legislation, statutory guidance and Trust policies, including Keeping Children Safe in Education (KCSIE).

Pupils will only be permitted to use generative AI where appropriate safeguards are in place, including suitable supervision, filtering, monitoring and age-appropriate controls.

For any use of AI, the Trust will:

- Comply with the Trust's AI Policy.

- Adhere to the age restrictions set by AI providers and open-access large language models (LLMs).

- Consider online safety risks when developing and implementing safeguarding policies and procedures.

- Refer to Keeping Children Safe in Education (KCSIE) to ensure AI tools are used safely and appropriately.

- Follow the Department for Education's guidance on generative AI product safety, filtering and monitoring standards.

- Ensure that personal, confidential and sensitive information is not entered into AI tools unless expressly authorised and appropriately protected.

The Trust will also prepare pupils to engage safely and responsibly with emerging technologies, including generative AI, by:

- Teaching pupils how to use AI safely, responsibly and in an age-appropriate manner.

- Helping pupils understand the limitations, risks and ethical considerations associated with AI-generated content.

- Taking reasonable steps to prevent pupils from accessing, generating or sharing harmful, inappropriate or misleading content through AI tools.

The Trust will maintain appropriate filtering and monitoring systems to reduce the risk of pupils accessing or creating harmful or inappropriate content using generative AI.

The Trust will continue to make use of relevant guidance, advice and best practice to ensure a safe, secure and reliable foundation is in place before adopting more advanced AI technologies.

20. Social Networking

Access to social networking sites is filtered and managed in accordance with the Trust's safeguarding and online safety requirements. Staff and pupils must not use social media for personal purposes during lesson time or other designated learning periods.

Staff should be aware that their conduct on social media, whether professional or personal, may have implications for their role and reputation, as well as that of the Trust. All staff are required to comply with the expectations set out in the Staff Code of Conduct regarding the appropriate use of social media.

Staff must not communicate with pupils or parents through personal social media accounts or social networking platforms. Staff are also expected to maintain appropriate privacy settings to minimise the risk of contact from pupils, parents or carers via social media.

Pupils are taught how to use social media safely, responsibly and respectfully through the Trust's online safety curriculum. This includes understanding online risks, protecting personal information, recognising inappropriate content and behaviour, and developing positive digital citizenship skills.

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

Use on behalf of the Trust

The Trust'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 Trust's social media accounts.

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

21. The Trust website

The headteacher is responsible for the overall content of the Trust 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

The Trust may issue staff with devices such as laptops, tablets and mobile phones to support them in carrying out their duties. Pupils may also be provided with Trust-owned devices where necessary to support teaching, learning and access to the curriculum.

All Trust-owned devices must be used in accordance with the applicable Acceptable Use Agreement and any related Trust policies.

The IT Department is responsible for managing and securing Trust-owned devices, including the deployment of software updates, security patches and antivirus protection. Staff and pupils must not install software, applications or other programmes without prior authorisation from the IT Department.

The Trust reserves the right to monitor and manage its devices to ensure their secure, appropriate and effective use.

Any misuse of Trust-owned devices by staff or pupils will be addressed in accordance with the relevant Trust policies, including the Staff Disciplinary Policy and Procedure and the

Behaviour Policy.

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 Trust'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 Trust.

Staff members may not use personal devices during lesson time, except 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 Trust 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 Trust of the expected use of personal devices. Any concerns about visitors' use of personal devices on the Trust 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 2027.

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

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

Appendix 1 – Online Safety Education

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) 2026.

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 **These rules will keep everyone safe.**

1. On-site, IT systems will be used for schoolwork and homework, I will store my schoolwork within my provided account on Microsoft Office 365 or 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 Trust 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 Trust day with the permission of a teacher.
6. I will not install or use VPNs on my device used in school. I accept that if I am found using a VPN, my device may be banned from the network or required to join the Trust's device management system.
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 a rude or 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 Trust in any way. We advise that you consider your digital footprint before posting anything online.
14. I will not download or install any software onto the IT Systems.
15. I will keep my logins, IDs and passwords secret, and only use my own login when accessing the Trust computers.
16. I will use the internet responsibly and will not visit websites I know to be banned by the Trust. I am also aware that during lessons, the staff will direct me to appropriate websites for my studies.
17. If a message from my antivirus software alerts me of a virus, I will report it to a teacher or the IT team 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 who has sent them.

23. I understand that all computer and internet use is monitored and recorded, which includes the use of remote screen monitoring software to ensure my safety and to support teaching and learning.
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, 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 hours.
30. I will only use current, officially supported operating systems from Apple, Android, and Microsoft. I will not use Linux or other operating systems unless I receive permission from the IT Department.
31. I will only use Microsoft Edge or Google Chrome as a web browser.
32. 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.
33. 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.
34. 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 able to spread infections to the network.
35. Electronic devices are brought into the Trust entirely at the risk of the owner, and the decision to bring the device into the Trust 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.
36. The Trust accepts no responsibility or liability in respect of lost, stolen or damaged devices while at school or on activities organised or undertaken by the Trust.
37. The Trust accepts no responsibility for any malfunction of a device due to changes made to the device while on the Trust network or whilst resolving any connectivity issues.
38. The Trust is not responsible for the day-to-day maintenance or upkeep of the users' personal devices, 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: _____

Appendix 3 - Acceptable Use Policy (Cranmore, Senior)

Pupil Acceptable Use Agreement **These rules will keep everyone safe.**

Digital technologies have become integral to the lives of children and young people, both within schools and outside school. These technologies are powerful tools, which open up new opportunities for everyone. These technologies can stimulate discussion, promote creativity and stimulate awareness of context to promote effective learning. Pupils should have an entitlement to safe internet access at all times.

This Acceptable Use Agreement is intended to ensure:

- that pupils will be responsible users and stay safe while using the internet and other digital technologies for educational, personal and recreational use.
- that school systems and users are protected from accidental or deliberate misuse that could put the security of the systems and users at risk.

Cranmore will try to ensure that pupils have good access to digital technologies to enhance their learning and will, in return, expect the pupils to agree to be responsible users.

These are the rules I agree to follow when using any digital technology:

1. I will not use my device/school computer for any purpose other than schoolwork or as directed by a member of staff whilst in school.
2. My device will be clearly labelled, charged up each evening and protected in a bag/case.
3. I understand that all computer and internet use is monitored and logged, which includes the use of remote screen monitoring software for the purpose of keeping me safe and to support teaching and learning.
4. I will only use current, officially supported operating systems from Apple, Android, and Microsoft. I will not use Linux or other operating systems unless I receive permission from the IT Department.
3. I will only use Microsoft Edge or Google Chrome as a web browser.
4. I will use only my own login and password, will not share my password with anyone, nor will I allow my school account to be used by anyone else.
5. I understand that all usage of the Trust computer systems is logged.
6. I shall use school-provided systems to save my work, i.e OneDrive from Office 365 or as directed by my teachers.
7. I will not save any personal information, including documents, images, or videos, on the Trust device or my school account.
8. To protect myself and other pupils, if I see anything I am unhappy with or receive messages I do not like, I will immediately close the page and tell a teacher or adult.
9. I will not access other people's files or send pictures of anyone without their permission.
10. I will not use my devices to take photos or video recordings during the Trust day without consent from a teacher.
11. I will not bring digital storage devices (e.g. USB storage) into school unless I have permission and they have been checked to ensure that they are virus-free.
12. I will only email people I know, or that my parent/teacher has approved, and the messages I send will be polite and sensible.

13. I will not give my home address or phone number or arrange to meet someone I have met online.
14. When I am using the internet to find information, I will check that the information is accurate, as I understand that the work of others may not be truthful or could have an ulterior motive.
15. Where work is protected by copyright, I will not try to download copies (including music and videos) or claim work to be my own (plagiarism).
16. I will not attempt to bypass the content filters or other security measures installed on the Trust's IT systems, and I will not attempt to access parts of the system that I do not have permission to access.
17. When on school premises, I will only access the internet through the Trust Wi-Fi; using personal data plans/tethered 4G or 5G mobile networks for access to the internet is expressly forbidden, as is the use of virtual private networks.
18. I will not attempt to install software on (unless through the Trust's Company Portal app) or otherwise alter the Trust IT systems.
19. I will not use my mobile phone in school for any reason. If I bring my phone to school, I will follow the Trust's procedure: switch it off and hand it in at the front Office.
20. I understand that the Trust may check my computer files.
21. If I am involved in incidents of inappropriate behaviour that involve members of the Trust community (e.g. cyber-bullying, using and/or sending images/video/information without permission), the Trust will take action according to the Behaviour Policy. This includes using social media during the Trust day.
22. I will not generate online posts (outside of official school-controlled outlets) using the Cranmore School name or branding or include a reference to pupils or staff.
23. I will not attempt to contact staff through social media or non-school-approved channels.
24. I understand that if I do not follow these rules, I may not be allowed to use ICT in school, my parents/carers may be contacted, and there may be sanctions in line with the Trust behaviour policy.
25. 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 able to infect the network.
26. Electronic devices are brought into the Trust entirely at the risk of the owner, as does the liability for any loss or damage resulting from the use of the device in school.
27. The Trust accepts no responsibility or liability in respect of lost, stolen or damaged devices while at school or on activities organised or undertaken by the Trust (the Trust recommends insurance is purchased to cover that device whilst out of the home).
28. The Trust accepts no responsibility for any malfunction of a device due to changes made to the device while on the Trust network or whilst resolving any connectivity issues.
29. The Trust is not responsible for the day-to-day maintenance or upkeep of the users' personal devices, such as the charging of any device, the installation of routine software updates or the resolution of hardware issues for devices where the device has not been purchased through the Trust.

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

Signed: _____ Date: _____

Name: _____ Form: _____

Appendix 4 - Acceptable Use Policy (Cranmore, Year 6)

Pupil Acceptable Use Agreement **These rules will keep everyone safe.**

Digital technologies have become integral to the lives of children and young people, both within schools and outside school. These technologies are powerful tools, which open up new opportunities for everyone. These technologies can stimulate discussion, promote creativity and stimulate awareness of context to promote effective learning. Pupils should have an entitlement to safe internet access at all times.

This Acceptable Use Agreement is intended to ensure:

- that pupils will be responsible users and stay safe while using the internet and other digital technologies for educational, personal and recreational use.
- that school systems and users are protected from accidental or deliberate misuse that could put the security of the systems and users at risk.

Cranmore will try to ensure that pupils have good access to digital technologies to enhance their learning and will, in return, expect the pupils to agree to be responsible users.

These are the rules I agree to follow when using any digital technology:

1. I will not use my device/school computer for any purpose other than schoolwork or as directed by a member of staff whilst in school.
2. My device will be clearly labelled, charged up each evening and protected in a bag/case.
3. I understand that all computer and internet use is monitored and recorded, which includes the use of remote screen monitoring software to ensure my safety and to support teaching and learning.
4. I will only use current, officially supported operating systems from Apple, Android, and Microsoft. I will not use Linux or other operating systems unless I receive permission from the IT Department.
3. I will only use Microsoft Edge or Google Chrome as a web browser.
4. I will ask permission from a teacher before using ICT equipment and will use only my own login and password.
5. I will not share my password with anyone, nor will I allow my school account to be used by anyone else.
6. I understand that all usage of the Trust computer systems is logged.
7. I shall use school-provided systems to save my work, i.e OneDrive from Office 365 or as directed by my teachers.
8. I will not save any personal information, including documents, images, or videos, on the Trust device or my school account.
9. To protect myself and other pupils, if I see anything I am unhappy with or receive messages I do not like, I will immediately close the page and tell a teacher or adult.
10. I will not access other people's files or send pictures of anyone without their permission.
11. I will not use my devices to take photos or video recordings during the Trust day without consent from a teacher.
12. I will not bring digital storage devices (e.g. USB storage) into school unless I have permission and they have been checked to ensure that they are virus-free.

13. I will only email people I know, or that my parent/teacher has approved, and the messages I send will be polite and sensible.
14. I will not give my home address or phone number or arrange to meet someone I have met online.
15. When I am using the internet to find information, I will check that the information is accurate, as I understand that the work of others may not be truthful or could have an ulterior motive.
16. Where work is protected by copyright, I will not try to download copies (including music and videos) or claim work to be my own (plagiarism).
17. I will not attempt to bypass the content filters or other security measures installed on the Trust's IT systems, and I will not attempt to access parts of the system that I do not have permission to access.
18. When on school premises, I will only access the internet through the Trust Wi-Fi; using personal data plans/tethered 4G or 5G mobile networks for access to the internet is expressly forbidden, as is the use of virtual private networks.
19. I will not attempt to install software on (unless through the Trust's Company Portal app) or otherwise alter the Trust IT systems.
20. I will not use my mobile phone in school for any reason. If I bring my phone to school, I will follow the Trust's procedure: switch it off and hand it in at the front Office.
21. I understand that the Trust may check my computer files.
22. If I am involved in incidents of inappropriate behaviour that involve members of the Trust community (e.g. cyber-bullying, using and/or sending images/video/information without permission), the Trust will take action according to the Behaviour Policy. This includes using social media during the Trust day.
23. I will not generate online posts (outside of official school-controlled outlets) using the Cranmore School name or branding or include a reference to pupils or staff.
24. I will not attempt to contact staff through social media or non-school-approved channels.
25. I understand that if I do not follow these rules, I may not be allowed to use ICT in school, my parents/carers may be contacted, and there may be sanctions in line with the Trust behaviour policy.
26. 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 able to infect the network.
27. Electronic devices are brought into the Trust entirely at the risk of the owner, as does the liability for any loss or damage resulting from the use of the device in school.
28. The Trust accepts no responsibility or liability in respect of lost, stolen or damaged devices while at school or on activities organised or undertaken by the Trust (the Trust recommends insurance is purchased to cover that device whilst out of the home).
29. The Trust accepts no responsibility for any malfunction of a device due to changes made to the device while on the Trust network or whilst resolving any connectivity issues.
30. The Trust is not responsible for the day-to-day maintenance or upkeep of the users' personal devices, such as the charging of any device, the installation of routine software updates or the resolution of hardware issues for devices where the device has not been purchased through the Trust.

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

Signed: _____ Date: _____

Name: _____ Form: _____

Appendix 5 - Acceptable Use Policy (Cranmore, Reception to Year 5)

Pupil Acceptable Use Agreement **These rules will keep everyone safe.**

Digital technologies have become integral to the lives of children and young people, both within schools and outside school. These technologies are powerful tools, which allow for new opportunities for everyone. These technologies can stimulate discussion, promote creativity and stimulate awareness of context to promote effective learning.

Young people should have an entitlement to safe internet access at all times.

This Acceptable Use Policy is intended to ensure:

- that young people will be responsible users and stay safe while using the internet and other digital technologies for educational, personal and recreational use.
- that school systems and users are protected from accidental or deliberate misuse that could put the security of the systems and users at risk.

Cranmore will try to ensure that pupils will have good access to digital technologies to enhance their learning and will, in return, expect the pupils to agree to be responsible users.

This is how I stay safe when I use computers:

- I will ask a teacher if I want to use the computers.
- I will not share my password with anyone, nor will I allow my school account to be used by anyone else.
- I will only use activities that a teacher has told or allowed me to use.
- I will take care of the computer and other equipment.
- I will ask for help from a teacher if I am not sure what to do or if I think I have done something wrong.
- I will tell a teacher if I see something that upsets me on the screen.
- I will not save any personal information, including documents, images, or videos, on the Trust device or my school account.
- I know that if I break the rules, I might not be allowed to use a computer.

Appendix 6 – Online Safety Policy for Boarding

Online Safety Policy for Boarding

Statement of Intent

Effingham Schools Trust recognises that boarding pupils have extended access to online technologies beyond the Trust day. In line with the National Minimum Standards for Boarding Schools, the Trust is committed to ensuring that boarders are safeguarded from harm and are supported to use technology safely, responsibly and respectfully at all times.

This appendix sets out the additional arrangements in place within boarding provision to promote a safe online environment and complements the EST Online Safety Policy and Safeguarding and Child Protection Policy.

1. Legal and Regulatory Framework

This appendix should be read in conjunction with the main policy and has due regard to:

- National Minimum Standards for Boarding Schools (particularly standards relating to safeguarding, welfare and supervision)
- Keeping Children Safe in Education 2026
- Online Safety Act 2023

The Trust ensures that arrangements for online safety in boarding reflect the expectation that boarders' welfare is safeguarded at all times, including outside the formal school day.

2. Scope

This appendix applies to:

- All boarding pupils
- All boarding staff
- Any devices used within boarding houses, whether school-owned or personal

3. Roles and Responsibilities

The Governing Board

The governing board ensures that:

- Boarding provision meets the expectations of the National Minimum Standards for Boarding Schools
- Appropriate filtering and monitoring systems extend to boarding environments
- Safeguarding arrangements for boarders include online safety outside teaching hours

The Headteacher

The headteacher ensures that:

- Online safety is embedded within boarding routines and expectations
- Boarding staff receive appropriate training in recognising and responding to online risks
- Clear systems are in place for managing device use in boarding

The DSL

The DSL:

- Maintains oversight of online safety concerns arising in boarding
- Ensures that safeguarding procedures are consistently applied across boarding and day provision
- Monitors trends in online incidents, including those occurring outside the Trust day

Boarding Staff

Boarding staff are responsible for:

- Promoting safe and responsible use of technology within boarding houses
- Maintaining appropriate supervision of pupils' welfare, including online activity
- Reporting concerns promptly in line with safeguarding procedures
- Modelling appropriate digital behaviours

4. Filtering and Monitoring

The Trust's filtering and monitoring systems apply across the boarding environment. As outlined in the EST Online Safety policy, all users are subject to monitoring when connected to the Trust network.

Within boarding:

- All devices connected to the Trust Wi-Fi are filtered and monitored
- Alerts generated outside school hours are reviewed and acted upon appropriately
- Boarding staff liaise with the DSL and IT staff where concerns arise

5. Use of Devices in Boarding

General Expectations

Pupils are expected to:

- Adhere to the Acceptable Use Policy at all times
- Use devices safely, responsibly and respectfully
- Avoid accessing or sharing harmful, inappropriate or illegal content

Boarding staff will intervene where device use presents a safeguarding concern.

Mobile Phone Access and Handover

The Trust provides clear guidance on when pupils are permitted to access mobile phones.

- Pupils are required to hand in devices at designated times, including overnight
- Devices are stored securely within boarding houses
- Access to devices is structured to promote:
 - pupil wellbeing
 - appropriate sleep routines
 - reduced risk of unsupervised online activity

Sixth Form Pupils

Pupils in the sixth form are permitted to retain their mobile phones overnight.

This reflects:

- Their age and stage of development
- A graduated approach to independence
- Preparation for responsible use of technology beyond school

Sixth form pupils remain subject to:

- The Acceptable Use Policy
- Safeguarding expectations
- Filtering and monitoring systems

6. Supervision and Pastoral Care

In accordance with the National Minimum Standards for Boarding Schools, appropriate supervision is maintained at all times.

Boarding staff:

- Remain vigilant to the risks associated with online activity during evenings and weekends
- Recognise that less structured time may increase exposure to online harm
- Provide support and guidance to pupils where concerns arise

Staff are trained to identify:

- Signs of cyberbullying
- Child-on-child abuse facilitated through technology
- Grooming or exploitation risks
- Changes in behaviour linked to online activity

7. Managing Online Safety Concerns in Boarding

All concerns are managed in line with the main policy and Safeguarding Policy.

Where concerns arise in boarding:

- They are reported to the DSL without delay
- Appropriate action is taken, including safeguarding intervention where required
- Incidents are recorded and monitored

Where necessary:

- Devices may be searched in line with statutory guidance
- Restrictions may be placed on device use
- Parents will be informed as appropriate

8. Education and Support

The Trust recognises that boarding provides additional opportunities to reinforce online safety education.

Boarding staff support pupils to:

- Develop healthy digital habits
- Understand the impact of online behaviour
- Manage screen time effectively
- Maintain respectful online relationships

This complements the curriculum outlined in the main policy .

9. Working with Parents

The Trust works in partnership with parents to support the online safety of boarders.

Parents are informed of:

- Expectations for device use in boarding
- Flexibility working with time scales and apps that are appropriate for our International pupils
- Arrangements for phone handover and supervision
- Any concerns relating to their child's online activity

10. Monitoring and Review

This appendix will be reviewed annually alongside the main EST Online Safety Policy.

It will also be reviewed in response to:

- Changes in statutory guidance
- Emerging risks in online safety
- Feedback from boarding staff, pupils and parents