Trumps Green Infant School

<u>Online and E-Safety Policy</u>

Trumps Green Infant School is committed to safeguarding, child protection and promoting the welfare of children and young people. We expect all members of the school community including staff, parents, carers, volunteers and governors to demonstrably share this commitment.

Introduction

E-safety is part of the school's safeguarding responsibilities. This policy should be seen in the context of our related policies on Computing, Acceptable Use Agreement, Behaviour, Staff Discipline, Anti bullying, data protection and our range of Safeguarding and Equality policies.

It is also part of the School Development Plan and has been written by the school, building on best practice and government guidance using the Surrey model policy. It has been agreed by senior management and approved by governors.

The purpose of this policy is to:

- Safeguard and protect all members of the school community in the use of computers and other devices and the internet.
- Identify approaches to educate and raise awareness of online safety throughout the schools community.
- Enable all staff to work safely and responsibly, to model behaviour online and to manage professional standards and practice when using technology
- Identify clear procedures to use when responding to online safety concerns

The E-safety policy covers the use of all technology which can access the school network and Internet or which facilitates electronic communication from school to beyond the bounds of the school site. This includes, but is not limited to, workstations, laptops, mobile phones and tablets used on the school site.

Roles
The school has nominated E-Safety Leaders being Sarah Morris and Janine Bond (Computing Lead and Sarah being Headteacher and DSL in addition) and a responsible member of the Governing Body (Helen Otter). The committee encourages input from all members of the school community to further e-safety practices.

<u>It is the responsibility of all members of staff to:</u>

- Contribute to the development of online safety procedures
- Read and adhere to the e-safety policy. Safeguarding and Child Protection policy, the ICT code of conduct /Acceptable Use Policy and the Staff Code of Conduct

<u>It is the responsibility of Governors to:</u>

- Undertake safeguarding and child protection training that includes online and E-Safety training.
- Read and adhere to this policy and to the school's Acceptable Use Policy

It is the responsibility of parents and carers to:

- Support the school in their online safety approaches by discussing online safety issues with their children and reinforce appropriate, safe online behaviours at home.
- Role model safe and appropriate use of technology and social media.
- Abide by the school's home-school agreement statements that relate to the use of social media and other e-safety issues.
- Identify changes in behaviour that could indicate that their child is at risk of harm online. If appropriate parents should inform the school for extra support and advice.
- Seek help and support from the school, or other appropriate agencies, if they or their child encounter risk or concerns online.
- Take responsibility for their own awareness in relation to the risks and opportunities posed by new and emerging technologies

Education and Engagement with pupils

The school will establish and embed a progressive online safety curriculum throughout the school to raise awareness and promote safe and responsible internet use amongst pupils by:

- Ensuring education regarding safe and responsible use precedes internet access.
- Including online safety in the Personal, Social and Health Education (PSHE) and Computing programmes of study, covering use both at home school and home.
- Reinforcing online safety messages whenever technology or the internet is in use.
- Educating pupils in the effective use of the internet to research; including the skills of knowledge location, retrieval and evaluation.
- Displaying acceptable use posters in all rooms with internet access and supporting pupils to read and understand it.

Vulnerable Pupils

- Trumps Green Infant School is aware that some pupils are considered to be more vulnerable online due to a range of factors. This may include, but is not limited to children in care, children with Special Educational Needs and Disabilities (SEND) or mental health needs, children with English as an additional language (EAL) and children experiencing trauma or loss.
- Trumps Green Infant School will ensure that differentiated and ability appropriate online safety education, access, monitoring and support is provided to vulnerable pupils.

Training and engagement with staff

The school will:

- Provide and discuss the online safety policy with all members of staff as part of induction.
- Provide a copy of the Online and E-Safety policy for all staff.

- Provide up-to-date and appropriate online safety training for all staff on a regular basis, with at least annual updates. To allow them to understand how digital technologies are used and are developing (particularly with learners) with regard to the areas defined in the KCSIE – content, contact, conduct and commerce. This training will be part of the annual safeguarding and child protection training or part of regular safeguarding updates throughout the year
- Make staff aware that school systems are monitored and activity can be traced to individual users; staff will be reminded to behave professionally and in accordance with school's policies when accessing school systems and devices.
- Make staff aware that their online conduct out of school, including personal use of social media, could have an impact on their professional role and reputation within school.
- Ensure all members of staff are aware of the procedures to follow regarding online safety concerns affecting pupils, colleagues or other members of the school community.

Awareness and engagement with parents and carers

Trumps Green Infant School recognises that parents and carers have an essential role to play in enabling children to become safe and responsible users of the internet and associated technologies. The school will build a partnership approach to online safety with parents and carers by:

- Providing information and guidance on online safety in a variety of formats. This will include offering specific online safety awareness training via the Safer School app, school website, newsletters and highlighting online safety at other events such as parent evenings.
- Drawing their attention to the school online safety policy, procedures and expectations.
- The school will ask all new parents to sign the parent/pupil agreement when they register their child with school.
- The school will send all parents a copy of the What's App usage policy at the start of each new academic year.

Reducing Online Risks

Trumps Green Infant School recognises that the internet is a constantly changing environment with new apps, devices, websites and materials emerging at a rapid pace. We will:

- Examine emerging technologies for educational benefit and a risk assessment will be carried out before use in school is allowed.
- Take all reasonable precautions to prevent access to inappropriate material. However, due to the international scale and linked Internet content, it is not possible to guarantee that unsuitable material will never appear on a school computer. Neither the school nor SCC can accept liability for the material accessed, or any consequences of Internet access.
- Staff will use a school phone where contact with pupils/parents is required.
- Ensure that appropriate filtering and monitoring is in place and take all reasonable precautions to ensure that users can only access appropriate material.
- The school will audit ICT use to establish if the E-safety policy is adequate and that the implementation of the E-safety policy is appropriate and effective.

Classroom Use

Trumps Green Infant School uses a wide range of technology. This includes access to:

- Computers, laptops, Smartboard and chrome books
- Apple iPads (2 per year group and 1 per teacher)
- Internet which may include search engines and educational websites
- Tablet and computer based applications and games
- Digital cameras
- Programmable Beebots and toys
- Staff will always evaluate websites, games and apps fully before being used in the classroom or being recommended for home use.
- The school will ensure that the use of internet-derived materials, by staff and pupils, complies with copyright law and acknowledge the source of information.
- Pupils' access to the internet will be by adult demonstration, with directly supervised access to specific and approved online materials, which support the learning outcomes planned for the pupils' age and ability.
- Pupils will be taught not to give out personal details or information which may identify them or their location.
- The school will provide an age-appropriate e-safety curriculum that teaches pupils how to stay safe, how to protect themselves from harm and how to take responsibility for their own and others' safety.

iPads
- All iPads remain the property of the school and are to only be used by class teachers, support staff and pupils. IPads must not be loaned to other adults or pupils without agreement from the Headteacher.
- All teacher iPad's storing pupil photographs or assessment data must be password protected and comply with the high standards of data protection.
- When left unattended, iPads must be locked in a secure place within a locked room. It is the responsibility of the class teacher to ensure all iPads are securely locked away.
- All apps must be approved by the Computing co-ordinator/head-teacher before being downloaded on the school iPads

Filtering and Monitoring

- The school Internet access is provided by Surrey County through the RM contract and includes filtering appropriate to the age of pupils.
- The school will work in partnership with Surrey County Council, RM and Soft Egg (technical support) to ensure systems to protect pupils are reviewed and improved.
- If staff or pupils come across unsuitable on-line materials, the site including the URL of the site if possible must be reported to the E-safety Coordinator. The breach will be recorded and escalated as appropriate. Parents/carers will be informed of filtering breaches involving their child.
- All staff are aware they can't rely on filtering and monitoring alone to safeguard pupils and that effective classroom management and regular education about online safe and responsible use is essential.
- Senior staff will ensure that regular checks are made to ensure that the filtering methods selected are appropriate, effective and reasonable.

Any material that the school believes is illegal will be reported immediately to the appropriate agencies, such as: Surrey Police or The Child Exploitation and Online Protection (CEOP)

Security and Management of Information Systems

The school takes appropriate action to ensure the security of our information systems, including:
- All Internet use by pupils will be supervised
- School ICT systems security will be reviewed regularly.
- Virus protection will be monitored and updated regularly.
- Security strategies will be discussed with the Local Authority.
- The appropriate use of user logins and passwords to access the school network
- All users are expected to log off or lock their screens/devices if systems are unattended.
- Not downloading unapproved software to work devices or opening unfamiliar email attachments. Any new software downloads have to be approved and agreed by Soft Egg.
- Systems will be put in place to ensure that internet use can be monitored and a log of any incidents will be kept to help identify patterns of behaviour and to inform online safety policy.
- All staff must read and sign the Acceptable Use Policy before using any school ICT resource. These should be returned to the Headteacher and stored in file
- The school will maintain a current record of all staff and pupils who are granted access to school ICT systems.
- Any person not directly employed by the school will be asked to sign an Acceptable Use of school ICT resources before being allowed to access the Internet from the school site.

Passwords

All members of staff will have their own unique username and private passwords to access school systems and Trumps Green school emails. Governors have their own username and private password to access Trumps Green school emails. Governors and members of staff are responsible for keeping their password private.
We require all users to:
- Use strong passwords for access into our systems
- Change passwords every 45 days. Users are prompted to do this.
- Always keep their password private; users must not share it with others or leave it where others can find it.
- Not to login as another user at any time.

Managing Email

- Any electronic communication which contains sensitive or personal information will only be sent using secure and encrypted emails.
- Teaching staff may only use approved e-mail accounts on the school system.
- Members of the school community will immediately tell the DSL if they receive offensive or unexpected e-mail and this will be recorded in the school safeguarding records.
- Pupils must not reveal personal details of themselves or others in e-mail communication, or arrange to meet anyone without specific permission.
- Incoming e-mail should be treated as suspicious and attachments not opened unless the author is known.

- The forwarding of chain letters is not permitted

Managing the Safety of the School Website

- The school will ensure that the information posted on our website meets the requirements as identified by the Department of Education (DfE) and OFSTED.
- The contact details on the Web site should be the school address, e-mail and telephone number. Staff, governors or pupil's personal information will not be published.
- The Headteacher or nominee will take overall editorial responsibility and ensure that content is accurate and appropriate.
- The school will post appropriate information about safeguarding, including online safety on the school website.
- The school website will comply with school's guidelines for publications including respect for intellectual property rights, privacy policies and copyright.
- Pupils' full names will not be used on the Web site, as appropriate, including in blogs, forums, press releases, news articles or wikis, particularly in association with photographs.
- Parents are asked to complete a blanket permission slip relating to use of photographs when their children start at TGIS.
- Parents should be clearly informed of the school policy on image taking and publishing, both on school and independent electronic repositories.

Managing Videoconferencing:

Video conferencing is a useful tool for staff to communicate with each other and to remotely teach pupils when necessary. When video conferencing with staff or pupils, the following guidelines will be adhered to:

- Videoconferencing will use the educational broadband network to ensure quality of service and security rather than the Internet.
- If a video conference is going to be recorded to be viewed again later, all people in the video conference will be informed before recording begins so that proper consent can be given.
- When screen-sharing during video conferencing, ensure that any documents being used on the computer of a confidential nature are not shown, or are closed prior to beginning screen sharing.
- Staff will be mindful of what can be seen and heard in the background when video conferencing, to make sure images and sounds are appropriate, non-offensive and do not breach individual privacy
- Video conferencing between staff will be accessed using accounts created with staff email addresses. All Child Protection, Safeguarding, Whistleblowing and Social Media Policies apply when working remotely using video conferencing.

Social Media

- The expectations' regarding safe and responsible use of social media applies to all members of Trumps Green Infant School community.

- The term social media may include, but is not limited to: blogs; wikis; social networking sites; forums; bulletin boards; online gaming; apps; video/photo sharing sites; chatrooms and instant messenger.
- All members of Trumps Green Infant School community are expected, at all times, to engage in social media in a positive, safe and responsible manner,
- The use of social media during school hours for **personal** use **is not** permitted.
- Concerns regarding the online conduct of any member of Trumps Green Infant School community on social media should be reported to the DSL and will be managed in accordance with the school's Anti-bullying, Allegations Against Staff, Behaviour and Safeguarding and Child protection policies.

Staff Personal Use of Social Media

- The safe and responsible use of social networking, social media and personal publishing sites will be discussed with all members of staff, governors and volunteers as part of induction and will be revisited and communicated via regular training opportunities for staff.
- All members of staff, governors and volunteers are advised that their online conduct on social media can have an impact on their role and reputation within school. Civil, legal or disciplinary action may be taken if they are found to bring the profession or institution into disrepute, or if something is felt to have undermined confidence in their professional abilities.
- All members of staff are advised to safeguard themselves and their privacy when using social media sites.
- Members of staff are encouraged not to identify themselves as employees of Trumps Green Infant School on their personal social networking accounts. This is to prevent information on these sites from being linked with the school and also to safeguard the privacy of staff members and governors.
- All members of staff are encouraged to carefully consider the information, including text and images, they share and post online and to ensure that their social media use is compatible with their professional role and is in accordance with schools policies and the wider professional and legal framework.
- Information and content that staff members have access to as part of their employment, including photos and personal information about pupils and their family members or colleagues will not be shared or discussed on social media sites.
- Members of staff will notify the DSL immediately if they consider that any content shared on social media sites conflicts with their role in the school.
- All members of staff are advised not to communicate with or add as 'friends' any current or past pupils or current or past pupils' family members via any personal social media sites, applications or profiles. Any pre-existing relationships or exceptions that may compromise this will be discussed with the Headteacher.
- Any communication received from pupils or parents on personal social media accounts will be reported to the DSL

Use of Personal Devices and Mobile Phones by staff and volunteers

Trumps Green Infant School recognises that personal communication through mobile technologies is an accepted part of everyday life for staff, governors, volunteers and parents/carers, but technologies need to be used safely and appropriately within school.

- Electronic devices of any kind that are brought onto site are the responsibility of the user at all times. The school accepts no responsibility for the loss, theft or damage of such items on school premises.
- The sending of abusive or inappropriate messages/ content via mobile phones or personal devices is forbidden by any member of the school community and any breaches will be dealt with as part of the school's codes of conduct and acceptable use policies.

Staff will be advised to:

- Keep mobile phones and personal devices in a safe and secure place during lesson time
- Keep mobile phones and personal devices switched off or switched to 'silent' mode during lesson times.
- Not use personal devices during teaching periods, unless written permission has been given by the Headteacher, such as in emergency circumstances.
- Ensure that any content bought onto site via mobile phones and personal devices are compatible with their professional role and expectations.
- Members of staff are not permitted to use their own personal phones or devices for contacting pupils or parents and carers.

Staff and governors will not use personal devices, such as: mobile phones, tablets or cameras:

- To take photos or videos of pupils and will only use school-provided equipment for this purpose.
- Directly with pupils, and will only use work-provided equipment during lessons/educational activities.
- If a member of staff or a governor is thought to have illegal content saved or stored on a mobile phone or personal device or have committed a criminal offence, the police will be contacted

Responding of Online Safety Incidents and Concerns

- All members of the school community will be made aware of the reporting procedure for online safety concerns, including: breaches of filtering, youth produced sexual imagery (sexting), cyberbullying and illegal content.
- All members of the community must respect confidentiality and the need to follow the official school procedures for reporting concerns.
- Pupils, parents and staff will be informed of the school's complaints procedure and staff will be made aware of the whistleblowing procedure.
- The school requires staff, parents, carers and pupils to work in partnership to resolve online safety issues.
- After any investigations are completed, the school will debrief, identify lessons learnt and implement any policy or curriculum changes as required.
- If the school is unsure how to proceed with an incident or concern, the DSL will seek advice from the Surrey Safeguarding Children Partnership.
- Where there is suspicion that illegal activity has taken place, the school will contact the Surrey Safeguarding Children Partnership or Surrey Police using 101, or 999 if there is immediate danger or risk of harm.
- If an incident or concern needs to be passed beyond the school community (for example if other local schools are involved or the public may be at risk), the school will speak with Surrey Police and/or the Surrey Safeguarding Children Partnership first, to ensure that potential investigations are not compromised.

Concerns about Pupils Welfare

- The DSL will be informed of any online safety incidents involving safeguarding or child protection concerns.
- The DSL will record these issues in line with the school's Safeguarding and child protection policy.
- The DSL will ensure that online safety concerns are escalated and reported to relevant agencies in line with the Surrey Safeguarding Children Partnership thresholds and procedures.
- The school will inform parents and carers of any incidents or concerns involving their child, as and when required.

Staff Misuse

- Any complaint about staff misuse will be referred to the DSL/Headteacher, according to the Management of Allegations and Concerns Safeguarding and child protection and Whistleblowing policies.
- Any complaint about the Headteacher's on-line misuse will be referred to the Chair of Governors according to the Management of Allegations and Concerns, Safeguarding and child protection and Whistleblowing policies.

Youth Produced Sexual Imagery or "Sexting"/now known as "sharing of nudes/semi nudes"

- Trumps Green Infant School recognises youth produced sexual imagery (known as "sexting") as a safeguarding issue; therefore all concerns will be reported to and dealt with by the Designated Safeguarding Lead.
- The school will follow the advice as set out in the non-statutory UKCCIS guidance: 'Sexting in schools and colleges: responding to incidents and safeguarding young people' and KSCB guidance: "Responding to youth produced sexual imagery".
- Trumps Green Infant School will ensure that all members of the community are made aware of the potential social, psychological and criminal consequences of 'sexting' by implementing preventative approaches, via a range of age and ability appropriate educational methods.
- The school will ensure that all members of the community are aware of sources of support regarding pupil produced sexual imagery.

Dealing with 'Sexting'

If the school are made aware of an incident involving the creation or distribution of pupil produced sexual imagery, the school will:

- Act in accordance with our Safeguarding and child protection policy and the relevant Surrey Safeguarding Child Partnership's procedures.
- Immediately notify the Designated Safeguarding Lead.
- Store the device securely.
- If an indecent image has been taken or shared on the school network or devices, the school will take action to block access to all users and isolate the image.

- Carry out a risk assessment which considers any vulnerability of pupil(s) involved; including carrying out relevant checks with other agencies.
- Inform parents and carers, if appropriate, about the incident and how it is being managed.
- Make a referral to Specialist Children's Services and/or the Police, as appropriate.
- Provide the necessary safeguards and support for pupils, such as offering counselling or pastoral support.
- Implement appropriate sanctions in accordance with the school's Behaviour policy, but taking care not to further traumatise victims where possible.
- Consider the deletion of images in accordance with the UKCCIS: 'Sexting in schools and colleges: responding to incidents and safeguarding young people' guidance.
- Images will only be deleted once the school has confirmed that other agencies do not need to be involved; and are sure that to do so would not place a child at risk or compromise an investigation.
- Review the handling of any incidents to ensure that best practice was implemented; the leadership team will also review and update any management procedures, where necessary.
- The school will take action regarding pupil produced sexual imagery, regardless of whether the incident took place on/off school premises, using school or personal equipment.

The school will not:
- View any images suspected of being pupil produced sexual imagery, unless there is no other possible option, or there is a clear need or reason to do so.
- In this case, the image will only be viewed by the DSL and their justification for viewing the image will be clearly documented.
- Send, share, save or make copies of content suspected to be an indecent image of children i.e. pupil produced sexual imagery and will not allow or request pupils to do so.

Online Child Sexual Abuse and Exploitation

- Trumps Green Infant School will ensure that all members of the community are aware of online child sexual abuse, including: exploitation and grooming; the consequences; possible approaches which may be employed by offenders to target children and how to respond to concerns.
- Trumps Green Infant School recognises online child sexual abuse as a safeguarding issue and, as such, all concerns will be reported to and dealt with by the Designated Safeguarding Lead.
- The school will implement preventative approaches for online child sexual abuse via a range of age and ability appropriate education for pupils, staff and parents/carers.
- The school will ensure that all members of the community are aware of the support available regarding online child sexual abuse, both locally and nationally.

Dealing with Online Child Sexual Abuse and Exploitation

If the school are made aware of incident involving online sexual abuse of a child, the school will:
- Act in accordance with the school's Safeguarding and child protection policy and the relevant Surrey Safeguarding Children Partnership's procedures.
- Immediately notify the Designated Safeguarding Lead.
- Store any devices involved securely.

- Immediately inform Surrey police via 101 (or 999 if a child is at immediate risk)
- Carry out a risk assessment which considers any vulnerabilities of pupil(s) involved (including carrying out relevant checks with other agencies).
- Inform parents/carers about the incident and how it is being managed.
- Make a referral to Specialist Children's Services (if required/ appropriate).
- Provide the necessary safeguards and support for pupils, such as, offering counselling or pastoral support.
- Review the handling of any incidents to ensure that best practice is implemented.
- Review and update any management procedures, where necessary.
- The school will take action regarding online child sexual abuse, regardless of whether the incident took place on/off school premises, using school or personal equipment.
- If the school is unclear whether a criminal offence has been committed, the DSL will obtain advice immediately through the Surrey Safeguarding Children Partnership and/or Surrey Police.
- If the school is made aware of intelligence or information which may relate to child sexual exploitation on or offline, it will be passed through to Surrey Police by the Designated Safeguarding Lead.
- If pupils at other schools are believed to have been targeted, the school will seek support from Surrey Safeguarding Children Partnership and/or Surrey Police first to ensure that potential investigations are not compromised.

Indecent Images of Children (IIOC)

- Trumps Green Infant School will ensure that all members of the community are made aware of the possible consequences of accessing Indecent Images of Children (IIOC).
- The school will take action regarding IIOC on school equipment and/or personal equipment, even if access took place off site.
- The school will take action to prevent accidental access to IIOC by using an internet Service provider (ISP) which subscribes to the Internet Watch Foundation block list and by implementing appropriate filtering, firewalls and anti-spam software.
- If the school is unclear if a criminal offence has been committed, the Designated Safeguarding Lead will obtain advice immediately through Surrey Safeguarding Children Board and/or Surrey Police.

If made aware of IIOC, the school will:
- Act in accordance with the schools child protection and safeguarding policy and the relevant Surrey Safeguarding Children Partnership procedures.
- Immediately notify the school Designated Safeguard Lead.
- Store any devices involved securely.
- Immediately inform appropriate organisations, such as Surrey police or the LADO.
- If made aware that a member of staff or a pupil has been inadvertently exposed to indecent images of children whilst using the internet, the school will:
- Ensure that the Designated Safeguard Lead is informed.
- Ensure that the URLs (webpage addresses) which contain the suspect images are reported to the Internet Watch Foundation via www.iwf.org.uk .
- Ensure that any copies that exist of the image, for example in emails, are deleted.
- Report concerns, as appropriate to parents and carers.

If made aware that indecent images of children have been found on the school devices, the school will:

- Ensure that the Designated Safeguard Lead is informed.
- Ensure that the URLs (webpage addresses) which contain the suspect images ar reported to the Internet Watch Foundation via www.iwf.org.uk .
- Ensure that any copies that exist of the image, for example in emails, are deleted.
- Inform the police via 101 (999 if there is an immediate risk of harm) and children's social services (as appropriate).
- Only store copies of images (securely, where no one else has access to them and delete all other copies) at the request of the police only.
- Report concerns, as appropriate to parents and carers.
- If made aware that a member of staff is in possession of indecent images of children on school devices, the school will:
- Ensure that the DSL/Headteacher is informed.
- Inform the Local Authority Designated Officer (LADO) and other relevant organisations in accordance with the school's Safeguarding and child protection, Managing of Allegations and Concerns and Whistleblowing policies.
- Quarantine any devices until police advice has been sought.

Cyberbullying

- Cyberbullying, along with all other forms of bullying, will not be tolerated at Trumps Green Infant School
- Full details of how the school will respond to cyberbullying are set out in the Anti-bullying policy.

Online Hate

- Online hate content, directed towards or posted by, specific members of the community will not be tolerated at Trumps Green Infant School and will be responded to in line with the school's Anti-bullying, Behaviour, Safeguarding and Child Protection and Whistleblowing policies.
- All members of the community will be advised to report online hate in accordance with relevant school policies and procedures.
- The Police will be contacted if a criminal offence is suspected.
- If the school is unclear on how to respond, or whether a criminal offence has been committed, the Designated Safeguarding Lead will obtain advice through the Surrey Safeguarding Children Partnership and/or Surrey Police.

Online Radicalisation and Extremism

- The school will take all reasonable precautions to ensure that children are safe from terrorist and extremist material when accessing the internet in school.
- If the school is concerned that a child or parent/carer may be at risk of radicalisation online, the DSL will be informed immediately and action will be taken in line with the Safeguarding and Child Protection Policy.
- If the school is concerned that member of staff may be at risk of radicalisation online, the DSL/ Headteacher will be informed immediately and action will be taken in line with the Safeguarding and Child Protection and Management of Allegations and Concerns Policies.

Protecting Personal Data:

- Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 1998.

Monitoring, Evaluation and Review

E-Safety is monitored in line with the Strategic School Development Plan policy monitoring cycle. The Governing Body monitors E-Safety within the school to evaluate its implementation and effectiveness.

Equality Statement

In accordance with our Equality Policy we will promote equality across the full range of protected characteristics and ensure that all pupils have equal access to all opportunities offered by the school.

Policy Status	
Agreed by Staff	September 2025
Next Review Date	September 2026