E-SAFETY POLICY

Our Vision:

We are committed to quality learning in a positive, happy and Christian atmosphere where everyone within the school community is valued as an individual. We expect everyone to, 'Treat others as you want them to treat you.' (Matthew 7:12-14). We have high expectations of all and strive to provide a safe, challenging, exciting and stimulating environment.

Our Values:

To prioritise the safety of children on-line, ensuring the highest standards of learning for all children, both at home and at school. These are met through our school values of:

- Respect – encourage and model the use of a range of technologies in a safe and respectful manner
- Compassion – use technologies with care and consideration for others.
- Creation – create regular and varied opportunities for children's learning to be enhanced and supported through the use of technology.
- Perseverance – embrace and use a range of technological approaches that support all children on their learning journey through school and beyond.
- Service – providing children with the necessary skills that enable them to flourish in a world full of technology.

At Willaston CE we aim to provide a caring, supportive and stimulating Christian environment with high quality care to promote the highest standards of e-safety for our whole school community.

E- Safety: The Rationale

E-Safety encompasses the use of new technologies, internet and electronic communications such as, mobile phones, video conferencing, collaboration tools and personal publishing. It highlights the need to educate pupils about the benefits and risks of using technology and provides safeguards and awareness for users to enable them to control their online experience.

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 the school; therefore, there are a number of 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 three areas of risk:

- **Content:** Being exposed to illegal, inappropriate or harmful material, e.g. pornography, fake news, and racist or radical and extremist views.
- **Contact:** Being subjected to harmful online interaction with other users, e.g. commercial advertising and adults posing as children or young adults.
- **Conduct:** Personal online behaviour that increases the likelihood of, or causes, harm, e.g. sending and receiving explicit messages, and cyberbullying.

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

Legal framework

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

- Voyeurism (Offences) Act 2019
- The General Data Protection Regulation (GDPR)
- Data Protection Act 2018
- DfE (2020) 'Keeping children safe in education'
- DfE (2019) 'Teaching online safety in school'
- DfE (2018) 'Searching, screening and confiscation'
- National Cyber Security Centre (2017) 'Cyber Security: Small Business Guide'
- UK Council for Child Internet Safety (2020) 'Education for a Connected World – 2020 edition'
- UK Council for Child Internet Safety (2017) 'Sexting in schools and colleges: Responding to incidents and safeguarding young people'

The Curriculum

Online safety is embedded throughout the curriculum;

- PSHE
- Computing
- RHE

The curriculum and the school's approach to online safety is developed in line with the UK Council for Child Internet Safety's 'Education for a Connected World' framework and the DfE's 'Teaching Online Safety in School' guidance.
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.

Online safety teaching is always appropriate to pupils' ages and developmental stages. The online safety teaching follows our school e-safety scheme of work. 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

The risks pupils may face online are always considered when developing the curriculum.

The DSL and Computing Lead are involved with the development of the school's online safety curriculum.

The school recognises that, while any pupil can be vulnerable online, there are some pupils who may be more susceptible to online harm or have less support from family and friends in staying safe online, e.g. pupils with SEND and LAC. Relevant members of staff, e.g. the SENCO, who is also the designated teacher for LAC ensures the curriculum is tailored so these pupils receive the information and support they need.

Class teachers review external resources prior to using them for the online safety curriculum, to ensure they are appropriate for the cohort of pupils. When reviewing these resources, the following questions are asked:

- Where does this organisation get their information from?
- What is their evidence base?
- Have they been externally quality assured?
- What is their background?
- Are they age appropriate for pupils?
- Are they appropriate for pupils' developmental stage?

External visitors may be invited into school to help with the delivery of certain aspects of the online safety curriculum. The Senior Leadership Team will decide when it is appropriate to invite external groups into school and ensure the visitors selected are appropriate.

Before conducting a lesson or activity on online safety, the class teacher and DSL/Computing Lead 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/Computing Lead 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 ensures a safe environment is maintained in which pupils feel comfortable to say what they feel 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 report it to the DSL/SLT and will log it onto CPOMS – taking the appropriate action in relation to the incident.

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 appropriate reporting procedures.

Staff training

All staff receive safeguarding training and sign an Acceptable Use document, which includes online safety training and advice, during their induction.

Online safety training for staff is updated when necessary, and is delivered in line with local and national guidance and advice.

In addition to this training, staff also receive online safety updates as required.

The DSL/Senior Leaders/Computing Lead undergo the appropriate training to provide them with the knowledge and skills they need to carry out their role.

In addition to any training, the DSL/Senior Leaders/Computing Lead receive regular online safety updates to allow them to keep up with any developments relevant to their roles. In relation to online safety, these updates allow the DSL/Senior Leaders/Computing Lead to:

- Understand the unique risks associated with online safety and be confident that they have the relevant knowledge and capability required to keep pupils safe while they are online at school.
- Recognise the additional risks that pupils with SEND face online and offer them support to stay safe online.

All staff receive a copy of this policy upon their induction and are informed of any changes to the policy.

Staff are required to adhere to the Teacher Standards at all times.

All staff are informed about how to report online safety concerns.

The Computing Lead acts as the first point of contact for staff requiring advice about online safety.

Educating Parents

The school works in partnership with parents to ensure pupils stay safe online at school and at home.

Parents are provided with information about the school's approach to online safety and their role in protecting their children. Parental awareness is raised in the following ways:

- Information on our School Website and Twitter Feed
- Newsletters, Letters and Leaflets
- Parent Workshops

Parents are sent a copy of the Responsible Internet Use document at the beginning of each academic year and are encouraged to go through this with their child to ensure their child understands the document and the implications of not following it.

Classroom use

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

- Computers
- Laptops
- Tablets
- Internet
- Email
- Programming Games and Tools

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 reviews and evaluates the resource.

Class teachers ensure that any internet-derived materials are used in line with copyright law.

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

Internet access

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

A record is kept of staff members who have signed this agreement and have been granted internet access in school.

All members of the school community are encouraged to use the school's internet network, instead of 3G, 4G and 5G networks, as the school network has appropriate filtering and monitoring to ensure individuals are using the internet appropriately.

Filtering and monitoring online activity

The Senior Leadership Team ensures the school's computing network has appropriate filters and monitoring systems in place.

The filtering and monitoring systems the school implements are appropriate to pupils' ages, the number of pupils using the network, how often pupils access the network, and the proportionality of costs compared to the risks.

The Computing Lead and Computing Technician ensure 'over blocking' does not lead to unreasonable restrictions as to what pupils can be taught with regards to online teaching and safeguarding.

The Computing Technician, with the support of the Computing Lead, undertakes regular checks on the filtering and monitoring systems to ensure they are effective and appropriate.

Requests regarding making changes to the filtering system are directed to the Headteacher.

Prior to making any changes to the filtering system, the Computing Lead, Computing Technician and the DSL conduct a risk assessment.

Any changes made to the system are recorded by the Computing Technician. Reports of inappropriate websites or materials are made to the Computing Lead, Computing Technician or DSL immediately, who investigates and records the matter and makes any necessary changes.

Deliberate breaches of the filtering system are reported to the Computing Lead, the DSL, Headteacher or Computing Technician, who will escalate the matter appropriately.

If a pupil has deliberately breached the filtering system, they will be disciplined in line with the Behavioural Policy.

If a member of staff has deliberately breached the filtering system, they will be disciplined in line with the Disciplinary Policy and Procedure.

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

The school's network and school-owned devices are appropriately monitored via Smoothwall

All users of the network and school-owned devices are informed about how and why they are monitored.

Concerns identified through monitoring are reported to the Computing Lead /Headteacher/DSL.

Network Security

Technical security features, such as anti-virus software, are kept up-to-date and managed by the Computing Technician.

Firewalls are switched on at all times.

The Computing Technician reviews the firewalls to ensure they are running correctly, and to carry out any required updates.

Staff and pupils are advised not to download unapproved software or open unfamiliar email attachments.

Staff members and pupils report all malware and virus attacks to the Computing Lead and Computing Technician.

All members of staff have their own unique usernames and private passwords to access the school's systems.

Pupils in class year or key stage and above are provided with their own unique username and private passwords.

Staff members and pupils are responsible for keeping their passwords private. 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. Users inform the Class Teacher or School Office if they forget their login details, who will arrange for the user to access the systems under different login details.

If a user is found to be sharing their login details or otherwise mistreating the password system, the Headteacher is informed and decides the necessary action to take.

Emails

Access to and the use of emails is managed in line with the Data Protection Policy, Acceptable Use Agreement and Confidentiality Policy.

Staff are given approved school email accounts and are only able to use these accounts at school and when doing school-related work outside of school hours. Prior to being authorised to use the email system, staff must agree to and sign the relevant Acceptable Use agreement.

Any email that contains sensitive or personal information is only sent using secure and encrypted email via Egress.

Staff members are required to block spam and junk mail, and report the matter to the Computing Technician.

The school's monitoring system can detect inappropriate links, malware and profanity within emails – staff and pupils are made aware of this.

Chain letters, spam and all other emails from unknown sources are deleted without being opened.

Social networking

Personal use

Access to social networking sites is filtered as appropriate.

Staff and pupils are not permitted to use social media for personal use during lesson time.

Staff can use personal social media during break and lunchtimes; however, inappropriate or excessive use of personal social media during school hours may result in the removal of internet access or further action.

Staff members are advised that their conduct on social media can have an impact on their role and reputation within the school.

Staff are not permitted to communicate with pupils or parents over social networking sites (not including Seesaw) and are reminded to alter their privacy settings to ensure pupils and parents are not able to contact them on social media (See Communication Policy).

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

Concerns regarding the online conduct of any member of the school community on social media are reported to the DSL/Headteacher and managed in accordance with the relevant policy, e.g. Anti-Bullying Policy, Staff Code of Conduct and Behavioural Policy.

Use on behalf of the school

The school's official Twitter account is only used for official educational or engagement purposes.

Staff members must be authorised by the Headteacher to access to the school's social media accounts.

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

The Acceptable Use Policy contains information on the acceptable use of social media – staff members are required to follow these expectations at all times.

The school website

The Headteacher and Office Staff are responsible for the overall content of the school website – they will ensure the content is appropriate, accurate, up-to-date and meets Government requirements.

The website complies with guidelines for publications including accessibility, data protection, respect for intellectual property rights, privacy policies and copyright law.

Personal information relating to staff and pupils is not published on the website. Images and videos are only posted on the website with prior consent from parents.

Use of school-owned devices

Staff members are issued with the following devices to assist with their work:

- Laptops
- Visualisers
- IPads.

Pupils are provided with school-owned devices as necessary to assist in the delivery of the curriculum, e.g. tablets to use during lessons.

School-owned devices are used in accordance with the Device User Agreement. Staff and pupils are not permitted to connect school-owned devices to public Wi-Fi networks.

All school-owned devices are fitted with software to ensure they can be remotely accessed, in case data on the device needs to be protected, retrieved or erased. ICT technicians review all school-owned devices to carry out software updates and ensure there is no inappropriate material on the devices.

No software, apps or other programmes can be downloaded onto a device without authorisation from ICT technicians.

Staff members or pupils found to be misusing school-owned devices are disciplined in line with the Disciplinary Policy and Procedure and Behavioural Policy.

Use of Personal Devices

Personal devices are used in accordance with the Acceptable Use Policy.

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

Personal devices are not permitted to be used in the following locations:

- Toilets

Only children in Year Six who walk to and from school independently, are permitted to bring a mobile phone to school, where they hand it to the class teacher until the end of the day. It will then be returned to the child on leaving the school premises.

In circumstances where a personal device has been brought into school without the agreement of school, the parents/carers of that child will be informed, and the incident will be recorded on CPOMS.

Staff members are not permitted to use their personal devices during lesson time, other than in an emergency.

Staff members are not permitted to use their personal devices to take photos or videos of pupils.

Staff members report concerns about their colleagues' use of personal devices on the school premises in line with dealing with Allegations of Abuse Against Teachers and Other Staff Policy.

If a member of staff is thought to have illegal content saved or stored on a personal device, or to have committed an offence using a personal device, the Headteacher will inform the police and action will be taken in line with the appropriate policies and procedures.

Pupils are not permitted to use their personal devices during lesson time.

If a pupil needs to contact their parents during the school day, they (or a staff member) must liaise with the school office.

If a staff member reasonably believes a pupil's personal device has been used to commit an offence or may provide evidence relating to an offence, the device will be handed to the police.

As visitors sign in at the office, they are informed of the expected use of personal devices.

Any concerns about visitors' use of personal devices on the school premises are reported to the Headteacher/DSL/Senior Leaders.

Managing reports of online safety incidents

Staff members and pupils are informed about what constitutes inappropriate online behaviour in the following ways:

- Staff training
- The online safety curriculum
- Assemblies
- Workshops

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. Staff Code of Conduct, Dealing with Allegations of Abuse Against Teachers and other Staff Policy and Disciplinary Policy and Procedures.

Concerns regarding a pupil's online behaviour are reported to the Headteacher/DSL who investigates concerns with relevant staff members, e.g. Computing Technicians. Concerns regarding a pupil's online behaviour are dealt with in accordance with relevant policies depending on their nature, e.g. Behavioural Policy and Safeguarding Policy.

Where there is a concern that illegal activity has taken place, the Headteacher contacts the police.

All online safety incidents and the school's response are recorded on CPOMS. The next section of this policy outlines how the school responds to specific online safety concerns, such as cyberbullying and peer-on-peer abuse.

Responding to specific online safety concerns

Cyberbullying

Cyberbullying, against both pupils and staff, is not tolerated.

Any incidents of cyberbullying are dealt with quickly and effectively whenever they occur.

Online sexual violence and sexual harassment between children (peer-on-peer abuse)

The school recognises that peer-on-peer abuse can take place online. Examples include the following:

- Non-consensual sharing of sexual images and videos
- Sexualised cyberbullying
- Online coercion and threats
- Unwanted sexual comments and messages on social media
- Online sexual exploitation

The school responds to all concerns regarding online peer-on-peer abuse, whether or not the incident took place on the school premises or using school-owned equipment.

Concerns regarding online peer-on-peer abuse are reported to the Headteacher/DSL/Senior Leaders who will investigate the matter in line with the Child Protection and Safeguarding Policy.

Upskirting

Under the Voyeurism (Offences) Act 2019, it is an offence to operate equipment and to record an image beneath a person's clothing without consent and with the intention of observing, or enabling another person to observe, the victim's genitals or buttocks (whether exposed or covered with underwear), in circumstances where their genitals, buttocks or underwear would not otherwise be visible, for a specified purpose.

A "specified purpose" is namely:

- Obtaining sexual gratification (either for themselves or for the person they are enabling to view the victim's genitals, buttocks or underwear).
- To humiliate, distress or alarm the victim.
- "Operating equipment" includes enabling, or securing, activation by another person without that person's knowledge, e.g. a motion activated camera.
- Upskirting is not tolerated by the school.

Incidents of upskirting are reported to the Headteacher/Senior Leaders/DSL who will then decide on the next steps to take, which may include police involvement, in line with the Safeguarding Policy.

Youth Produced Sexual Imagery (Sexting)

Youth produced sexual imagery is the sending or posting of sexually suggestive images of under-18s via mobile phones or over the internet. Creating and sharing sexual photos and videos of individuals under 18 is illegal.

All concerns regarding sexting are reported to the Headteacher/Senior Leaders/DSL. Following a report of sexting, the following process is followed:

- The DSL holds an initial review meeting with appropriate school staff
- Subsequent interviews are held with the pupils involved, if appropriate
- Parents are informed at an early stage and involved in the process unless there is a good reason to believe that involving the parents would put the pupil at risk of harm
- At any point in the process if there is a concern a pupil has been harmed or is at risk of harm, a referral will be made to IART and/or the police immediately
- The interviews with staff, pupils and their parents are used to inform the action to be taken and the support to be implemented

When investigating a report, staff members do not view the youth produced sexual imagery unless there is a good and clear reason to do so.

If a staff member believes there is a good reason to view youth produced sexual imagery as part of an investigation, they discuss this with the Headteacher first.

The decision to view imagery is based on the professional judgement of the Headteacher/Senior Leaders/DSL and always complies with the Safeguarding Policy.

Any accidental or intentional viewing of youth produced sexual imagery that is undertaken as part of an investigation is recorded.

If it is necessary to view the imagery, it will not be copied, printed or shared.

Online Abuse and Exploitation

Through the online safety curriculum, pupils are taught about how to recognise online abuse and where they can go for support if they experience it.

The school responds to concerns regarding online abuse and exploitation, whether or not it took place on the school premises or using school-owned equipment.

All concerns relating to online abuse and exploitation, including child sexual abuse and exploitation and criminal exploitation, are reported to the

DSL/Headteacher/Senior Leaders and dealt with in line with the Child Protection and Safeguarding Policy.

Online Hate

The school does not tolerate online hate content directed towards or posted by members of the school community.

Incidents of online hate are dealt with in line with the relevant school policy depending on the nature of the incident and those involved, e.g. Staff Code of Conduct, Anti-Bullying Policy.

Online Radicalisation and Extremism

The school's filtering system protects pupils and staff from viewing extremist content. Concerns regarding a staff member or pupil being radicalised online are dealt with in line with the Safeguarding Pupils Vulnerable to Extremism Policy.

Remote learning

All remote learning is delivered in line with the school's Pupil Remote Learning Policy and On-line Video / Live Learning Session Protocol.

All staff and pupils using video communication must:

- Communicate in groups – one-to-one sessions are only carried out where necessary.
- Wear suitable clothing – this includes others in their household.
- Be situated in a suitable 'public' living area within the home with an appropriate background – 'private' living areas within the home, such as bedrooms, are not permitted during video communication.
- Use appropriate language – this includes others in their household.
- Maintain the standard of behaviour expected in school.
- Use the necessary equipment and computer programs as intended.
- Not record, store, or distribute video material without permission.
- Ensure they have a stable connection to avoid disruption to lessons.
- Always remain aware that they are visible.

Pupils not using devices or software as intended will be disciplined in line with the Behaviour Policy.

The school will risk assess the technology used for remote learning prior to use and ensure that there are no privacy issues or scope for inappropriate use.

The school will ensure that all school-owned equipment and technology used for remote learning has suitable anti-virus software installed, can establish secure connections, can recover lost work, and allows for audio and visual material to be recorded or downloaded, where required.

The school will communicate to parents in writing about any precautionary measures that need to be put in place if their child is learning remotely using their own/family-owned equipment and technology.

During the period of remote learning, the school will maintain regular contact with parents to:

- Reinforce the importance of children staying safe online.
- Ensure parents are aware of what their children are being asked to do, e.g. sites they have been asked to use and staff they will interact with.
- Encourage them to set age-appropriate parental controls on devices and internet filters to block malicious websites.
- Direct parents to useful resources to help them keep their children safe online.

The school will not be responsible for providing access to the internet off the school premises and will not be responsible for providing online safety software, e.g. anti-virus software, on devices not owned by the school.

Monitoring and review

The school recognises that the online world is constantly changing; therefore, the DSL, ICT technicians and the Headteacher conduct half-termly light-touch reviews of this policy to evaluate its effectiveness.

The Governing Body, Headteacher and DSL review this policy in full on an biennial basis and following any online safety incidents.

The next scheduled review date for this policy is July 2023.

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

Approved by Governors July 2021

Signed Chair of Governors

Appendix 1

Responsible Internet Use

We use the computers and internet connection for learning. These rules will help us be fair to others and keep everyone safe.

- **I will ask permission before entering any website, unless my teacher has already approved that site.**
- **On a network, I will use only my own login and password, which I will keep secret, or the login and password given by my teacher.**
- **I will not look at or delete other people's files.**
- **I will not bring computer disks or memory sticks into school without permission.**
- **I will only send e-mails which my teacher has approved.**
- **The messages I send will be polite and sensible.**
- **When sending an e-mail, I will not give my home address or phone number, or arrange to meet someone.**
- **I will ask for permission before opening an e-mail or an e-mail attachment.**
- **I will not use internet chat.**
- **If I see anything I am unhappy with or I receive messages I do not like, I will tell a teacher immediately.**
- **I know that the school may check my computer files and may monitor the internet sites I visit.**
- **I understand that if I deliberately break these rules, I could be stopped from using the internet or computers.**

The school may exercise its right by electronic means to monitor the use of the school's computer system, including the monitoring of web-sites, the interception of e-mail and the deletion of inappropriate materials in circumstances where it believes unauthorised use of the school's computer system is or may be taking place, of the system is or may be being used for criminal purposes or for storing text or imagery which is unauthorised or unlawful.