E-SAFETY POLICY

Personnel and Curriculum Committee ☐

Finance and Premises Committee ☐

Full Governing Body ☑

Headteacher **(Sam Brunt)**	**Signature** *S Brunt*
Chairperson **P Ananicz**	**Signature** *P Ananicz*

Date ratified: 21.1.26

Review date: Spring Term 2029

St. Augustine's Junior C of E (VA) Junior School
E-safety Policy

Acceptable Use of ICT and E-safety

At St Augustine's CE Junior School, we recognise that information and communication technology play an important part in learning. All learners in school must use technology appropriately, safely and legally. We have a responsibility to make all learners aware of the appropriate behaviours' and critical thinking skills to enable them to remain both safe and legal when using the internet and related technologies. This policy is linked, and works alongside the school's ICT, child protection and anti-bullying policies.

Responsibility for E-safety and Appropriate use of ICT

The school governing body has responsibility for ensuring that the school has an Acceptable use Policy for ICT and this policy is reviewed annually.

The Head teacher will ensure that there is a designated person for coordinating e-safety and acceptable use of ICT. The ICT co-ordinator will work closely with the designated person for child protection.

The day-to-day duty of online safety officer is devolved to: Alessandro Corbino

The online safety officer will:

- Lead the online safety committee
- Keep up to date with the latest risks to children whilst using technology; familiarise him/ herself with the latest research and available resources for school and home use.
- Take day-to-day responsibility for online safety issues, has a leading role in establishing and reviewing this policy regularly along with other related document, and bring any matters to the attention of the Head teacher.
- Advise the Head teacher, governing body on all online safety matters.
- Meets with the online safety governor regularly meets regularly to discuss current issues, review incident logs and filtering / change control logs.
- Provides training and advice for staff and ensures that all staff are aware of the procedures that need to be followed in the event of an online safety incident-taking place.
- Retain responsibility for the online safety incident log, ensure staff know what to report and ensure the appropriate audit trail as well as a log of incidents to inform future online safety developments. SEE APPENDIX 5
- Engage with parents and the school community on online safety matters at school and/or home.
- Liaise with the local authority, IT technical support and other agencies as required.
- Ensure any technical online safety measures in school (e.g. internet filtering software, behaviour management software) are fit for purpose through liaison with the LA and ICT technical support.

- Make him/ herself aware of any reporting function with technical online safety measures, i.e. internet filtering reporting function, liaise with the Head teacher and responsible governor to decide on what reports may be appropriate for viewing.
- Reports regularly to the Senior Leadership Team and in partnership with them decides on the investigation/action and sanctions process for any online safety incidents.

All staff have a responsibility to use ICT appropriately and legally. They also have a duty to report any illegal or inappropriate use of ICT to the head teacher or the designated person for e-safety, as soon as possible.

Teachers and teaching assistants should address issues of e-safety when using the internet with children. All children must follow all the ICT Code of Conduct (see appendix 1).

The ICT support team will ensure that computers have up to date virus protection and internet connection is filtered through the regional broadband consortium.

Use of the Internet

The school encourages users to make effective use of the Internet. Such use should always be lawful and appropriate. Internet usage means any connection to the Internet via Web browsing, Google Apps for Education, Gmail or Apps approved and designated by the school.

The school expects all users to use the Internet responsibly and strictly according to the following conditions:

Users shall **not** visit internet sites, make, post, download, upload or pass on, material, remarks, proposals or comments that contain or relate to:

- pornography (including child pornography)
- promoting discrimination of any kind
- promoting racial or religious hatred
- promoting illegal acts
- any other information which may be considered offensive to colleagues

Incidents which appear to involve deliberate access to Web sites, newsgroups and online groups that contain the following material will be reported to the police:

- images of child abuse (images of children, apparently under 16 years old) involved in sexual activity or posed to be sexually provocative
- adult material that potentially breaches the Obscene Publications Act in the UK
- criminally racist material in the UK

If inappropriate material is accessed accidentally, users should immediately report this to the Head teacher or designated e-safety coordinator so appropriate action can be taken.
Children that access material that concerns them should close the lid of the laptop/ Chromebook and consult their teacher. The teacher will then report the material to the ICT co-ordinator or Head teacher who will then contact our ICT support (provided by Ark) who will then liaise with Talk Straight.

System Monitoring & Filtering

Our broadband is provided through Talk Straight and thus all web filtering meets government and BECTA standards. All internet access provided to staff and children is strictly filtered through the broad band consortium.

In addition, Securus is used to monitor adults' and children's use of internet and devices at St Augustine's.

Data Protection and System security

All users on the system are expected to protect their own login details (for Google accounts and related educational apps) as a matter of personal and system security. Under no circumstance should people allow other users to have their details or use their login. If at any time a user feels that their password has been seen by another user, they should log on and change their password immediately. It is also recommended that all passwords are alphanumeric. Staff are required to change their password for their laptop every 90 days – a reminder is sent through their laptop system. At the same time, staff should change their Google password too.

User personal and system security code of conduct:

- Any person logging on or accessing google apps for education or the school network should only use their own unique username and password. Under no circumstances should these be shared with others.

- By allowing others to use your details you will put yourself at risk of being wrongly accused of another child's impropriety. It will also negate the monitoring integrity as we will not be able to guarantee that the user was responsible for the inappropriate use unless we can guarantee everyone is using their login details only.

- When entering password on a website login or the platform you will often be asked if you would like to save your details. Children are told never to save their details on a school computer, only to their own personal computer.

- The school network and Google Apps for Education does contain secure student detail and staff documentation. If any details are seen by another person this data could be compromised. If in doubt, the password needs to be changed immediately.

- If accessing school data from home on a personal or school provided hardware, it should always be ensured, by following the aforementioned code that data integrity is respected at all times. All equipment is more vulnerable once it leaves the building. Laptops and mobile technology are susceptible to theft and loss along with its data.

- A guest login will be provided for visitors to access the internet.

Digital Media

Digital media and photographs play an important part of recording events in school life. School provides iPads for use by children and staff. Personal devices should not be used. School provides iPads and a smartphone for adults which should be used for taking photographs and uploading to Class Dojo. The uploading of photographs complies with school GDPR policies. If a staff member records images, then the images should only be downloaded onto the school network for storage and deleted from the school iPad or smartphone as soon as possible.

Staff/Governors Email

All email messages should include a standard disclaimer stating that the content of the email are not necessarily the views of school or LA. Unsolicited email with children is not allowed. Any communication with children via email should be through the staff school email account to the pupil school account only (e.g. sharing of work via Google Drive.) Do not release or in any way make available personal details of any colleague or pupil (phone numbers or personal e-mail addresses) over the Internet.
Governors should use their school email accounts as opposed to personal email addresses.

Mobile Phones

Children are not allowed mobile phones in school and should be placed in the lock box in their classrooms for safekeeping if they are brought into school. This box is taken down to the office for safekeeping and collected again at the end of the day for children to take their phones home.

Internet Games

There are times in the week when children may have 'free' use of the school network, such as during wet playtimes, reward time for good behaviour etc. Any games played on the school network must be in line with the school Code of Conduct and be suitable for primary aged children - staff are responsible for ensuring games are appropriate.

Downloading Files such as Music, Videos or Games

Children should not download any files onto the school network. If files such as music, videos or games are free to download they are usually illegal. Staff may download music but this must be done legally and in line with copyright laws.

Internet safety skills for pupils

ICT Code of Conduct (see appendix 1) will be referred to in the Home School Agreement. Pupils should be reminded of internet safety rules when using the Internet. After the first Internet Safety lesson of the new school year, children will be asked to sign the Code of Conduct, which is then sent home for parents to read, sign and return to school.

Pupils will be taught about online safety as part of the curriculum.
Pupils in **Key Stage 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

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

- That people sometimes behave differently online, including by pretending to be someone they are not
- That the same principles apply to online relationships as to face-to-face relationships, including the importance of respect for others online including when we are anonymous
- The rules and principles for keeping safe online, how to recognise risks, harmful content and contact, and how to report them
- How to critically consider their online friendships and sources of information including awareness of the risks associated with people they have never met

- How information and data is shared and used online
- What sorts of boundaries are appropriate in friendships with peers and others (including in a digital context)
- How to respond safely and appropriately to adults they may encounter (in all contexts, including online) whom they do not know

Social Networking

The use of personal Instagram, Facebook and other social networking sites is prohibited at school. Unsolicited contact between staff members and children (past or present) is not allowed. It is also prohibited to use any recognisable images of any child that attends the school on a personal social networking site.

The school has a Facebook and Instagram account that is able to be viewed by the general public. We ensure any image file is appropriately named – do not use pupils' names in image file names or ALT tags if published on the web. This reduces the risk of inappropriate, unsolicited attention from people outside school. We will use group photos rather than photos of individual children, wherever possible.

Sanctions

Sanctions will be appropriate to the seriousness of the offence. For example temporary suspension of ICT rights for minor offences, ranging to permanent exclusion and involvement of the police for very serious offences.

School website

Any work published on the school website is thoroughly checked to ensure that there is no content that compromises the safety of pupils or staff. The school will obtain parental permission before using images of pupils on the website, in line with our GDPR policy. We ensure the image file is appropriately named – do not use pupils' names in image file names or ALT tags if published on the web. This reduces the risk of inappropriate, unsolicited attention from people outside school. We will use group photos rather than photos of individual children, wherever possible. Images will be appropriately stored and secured on the school's network.

This policy will be reviewed yearly and updated annually. It will form part of induction for all new staff, and will also be referred to in the Home School Agreement.

APPENDIX 1: Code of Conduct for Children (ICT Guidelines)

Always ask an adult
Only use the Internet with adult permission and with an adult present in the room.

Never give anyone your personal details.
Never give any information which would help anyone work out where you live or who you are. Don't give out details about your daily routine (where you go, what you do at what times). You would not give your name and address to a stranger you meet at a bus stop. So do not give your full name, telephone number or address when working on the Internet. The same applies about giving information about your family and friends.

Do not arrange to meet people through the Internet.
Remember, not everyone you 'meet' on-line are who they say they are. People can pretend to be someone else. Tell an adult if someone you don't know contacts you.

Do not look for things on the internet that are rude, racist or illegal.
If you deliberately write or look at something that is rude, racist or illegal a screenshot (photo of your page) will be immediately sent to the server that is monitored by the ICT coordinator and Head teacher.

Ask 'Is it true?'
Just because it comes out of a computer does not mean it is true! Some people make up things. Always check where the information has come from and check it. Can you trust it? Rule of 3 – if the same piece of information can be found on 3 different, trusted websites, it can usually be trusted.

Never delete, change or read other people's emails, files or passwords.
We share our network so remember to be careful. You do not want your work deleted or changed, so don't do it to others. Never attempt to log on as somebody else.

Do not play computer games that are not suitable for school.

If you are playing games, make sure they are in line with the schools Code of Conduct – we don't have fighting in school, so don't play games that involve fighting. Don't play games which are violent or are meant for older children or adults. Ask an adult if you are unsure about a game.

Do not download, listen to or watch music or videos.
If music/videos are free to download then it is usually illegal. Don't listen to music or watch videos in school that are rude, racist or meant for older children or adults. Always ask an adult.

What to do if you see something that concerns you
It is likely that at some point you will come across some images or words that you did not intend to see. If this happens and you do see or hear something that scares, worries or upsets you do the following immediately.
• Close the lid of the laptop. Do not turn the PC off.
• Tell an adult immediately.
• DO NOT show other students what you have seen or discuss with them.
The adult will then copy the URL and notify the ICT coordinator. You will NOT get blamed.

Appendix 2: Pupil's Acceptable Use Agreement

Name of child: ……

I understand that using the computer network at St Augustine's Junior School is a privilege which could be taken away from me, unless the E-Safety rules are followed.

E-Safety Rules

When using the iPads and chrome books I will:

- Be **SMART** online and **STOP** and **THINK** before **I CLICK**.
- Never enter my address, telephone number, photographs, videos or any other details (such as daily routine or location) about me or anyone else.
- Always tell an adult if something or someone online makes me feel uncomfortable or upset.
- Remember that people online may not be who they say they are and I will tell an adult if someone I do not know contacts me.
- Not post photographs or videos without an adult's permission as I understand these can be manipulated and may attract the wrong sort of attention.
- Always behave sensibly, respecting other members of the school.
- Only log in using my own username and password.
- Never access or distribute any material on the network which may upset/be considered offensive by others.
- Report any upsetting/offensive messages or images that I may receive in error through the network to my class teacher or Head teacher.
- Not waste my time playing non-educational games.
- Not download any games/music/videos or other programs without the permission of my class teacher.
- Only enter the school contact details on a website e.g. address, telephone number with explicit permission of my class teacher.
- Not leave inappropriate comments on any social media or learning platform pages that I have access to (e.g. Class Dojo, SeeSaw etc).

If I break any of these rules or see anyone breaking the rules, I will report it to my teacher immediately and realise that I may face consequences from my actions, but that my honesty will be recognised.

Child

I have read the E-Safety Rules and will follow them. I agree to the 'Pupil's Acceptable Use Agreement'.

Signed: …… Date: ……

Parent/carer

I understand that the school will do its utmost to ensure the suitability of content that the children are exposed to at school. However, I acknowledge that at some point, when learning how to safely use ICT at school, my child may come across something that is deemed inappropriate. In such cases, my child will know how to deal appropriately with the situation following the E-Safety Rules. I understand that my child will not be allowed to use ICT in school until this agreement has been signed and returned.

I acknowledge the 'Pupil's Acceptable Use Agreement' and support the school in its efforts to keep children safe when using technology and the internet in school.

Signed: …… Date: ……

Appendix 3: Staff E-Safety Acceptable Use Agreement

To be included in the annual safeguarding training.

Use of school based equipment

When using the school's ICT equipment and other information systems, I have understood and will comply with the following statements

- I will access the internet and other ICT systems using an individual username and password, which I will keep secure. I will ensure that I log out after each session and never allow other users to access the internet through my username and password. I will report any suspicion, or evidence that there has been a breach of my personal security in relation to access to the internet or ICT systems, to the e-safety coordinator.
- All passwords I create will be in accordance with the school e-safety Policy. I will ensure that I use a suitably complex password for access to the internet and ICT systems.
- I will not share my passwords.
- I will seek consent from the e-safety coordinator/ headteacher prior to the use of any new technologies (hardware, software, cloud-based services) within school.
- I will not search for, download, upload or forward any content that is illegal or that could be considered an offence by another user. If I encounter any such material I will report it immediately to the e-safety coordinator/ Headteacher.
- I will take a professional and proactive approach to assessing the effectiveness of the internet content-filtering platform in relation to the educational content that can be viewed by the pupils in my care.
- I will not attempt to bypass any filtering and/or security systems put in place by the school. If I suspect a computer or system has been damaged or affected by a virus or other malware, I will report this to the network manager / e-safety coordinator (as appropriate)
- I understand my personal responsibilities in relation to the Data Protection Act and the privacy and disclosure of personal and sensitive confidential information.
- I will take reasonable precautions to ensure that any devices (laptops, tablets, cameras, removable media or phones) are stored in a secure manner when taken off site (car / home/ other location). Devices will not be stored in a car overnight or left in sight when not in use, e.g. by an open window or on the back seat of a car.
- I will only use school-owned SD cards.
- I will ensure that any personal or sensitive information taken off site will be situated on a school-owned device with appropriate technical controls such as encryption/ password protection deployed.
- Any information asset, which I create from other information systems, which could be deemed as personal or sensitive will be stored on the school network and access controlled in a suitable manner in accordance with the school data protection controls. (For example spread sheets/other documents created from information located within the school information management system).
- I will not download or install any software from the internet or from any other media which may compromise the school network or information situated on it without prior authorisation from the network manager.

- I understand that the use of computer systems without permission or for inappropriate purposes could constitute a criminal offence under the Computer Misuse Act 1990 and breaches will be reported to the appropriate authorities.
- I understand that my files, communications and internet activity may be monitored and checked at all times to protect my own and others' safety, and action may be taken if deemed necessary to safeguard me or others.

Social Networking

- I must not talk about my professional role in any capacity when using personal social media such as Facebook, Instagram and YouTube or any other online publishing websites.
- I must not use social media tools to communicate with current or former pupils under the age of 18.
- I will not use any personal social media tools to communicate with parents unless approved by the Head Teacher.
- I will set and maintain my profile on social networking sites to maximum privacy and give access to known friends only.
- Staff must not access social networking sites for personal use during school hours.
- If I experience any derogatory or slanderous comments relating to the school, colleagues or my professional status, I will take screenshots for evidence and escalate to the e-safety coordinator.

Managing digital content

- I will demonstrate professional, safe and responsible behaviour when creating, using and storing digital images, video and sound within school.
- I will only use school equipment to create digital images, video and sound. Digital images, video and sound will not be taken without the permission of participants; images and video will be of appropriate activities and participants will be in appropriate dress. No resources will be published online without the permission of the staff and pupils involved as detailed in the e-safety Policy/ Data Protection Policy.
- Under no circumstances will I use any personally-owned equipment for video, sound or images.
- When searching for images, video or sound clips, I will ensure that I or any pupils in my care are not in breach of any copyright licencing.
- I will ensure that any images, videos or sound clips of pupils are stored on the school network and never transferred to personally-owned equipment.
- I will ensure that any images taken on school-owned devices will be transferred to the school network (storage area/server) and deleted as soon as possible from the memory card.
- I will model safe and responsible behaviour in the creation and publishing of online content within the school learning platform and any other websites. In addition to this I will encourage colleagues and pupils to adopt similar safe behaviour in their personal use of blogs, wikis and online publishing sites.

Email

- I will use my school email address for all correspondence with staff, parents or other agencies and I understand that any use of the school email system will be monitored and checked. I will under no circumstances use my private email account for any school-related business.
- Communication between staff and pupils or members of the wider school community should be professional and related to school matters only.
- I will ensure that any posts made on websites or via electronic communication, by either myself or the pupils in my care, will not damage the reputation of my school.
- I will seek permission if I need to synchronise any school email account with a personally-owned handheld device.
- I will take care in opening any attachments sent by email. I will only open emails and associated attachments from trusted senders.
- Emails sent to external organisations will be written carefully and if necessary authorised before sending to protect myself. As and when I feel it necessary, I will carbon copy (cc) the head teacher, line manager or another suitable member of staff into the email.
- I will ensure that I manage my email account, delete unwanted emails and file those I need to keep in subject folders.
- I will access my school email account on a regular basis to ensure that I respond in a timely manner to communications that require my attention.

Mobile phones and devices

- I will ensure that my mobile phone and any other personally-owned device is switched off or switched to 'silent' mode during school hours.
- Bluetooth communication should be 'hidden' or switched off and mobile phones or devices will not be used during teaching periods unless permission has been granted by a member of the Senior Leadership Team in emergency circumstances.
- If contacting any parents or pupils on my personally-owned device, I will ensure my number is hidden.
- I will not use any personally-owned mobile device to take images, video or sound recordings unless required in special/emergency circumstances or agreed with the head teacher beforehand.

Learning and teaching

- In line with every child's legal entitlement I will ensure I teach an age appropriate e-safety curriculum.
- I will support and promote the school e-safety policy at all times. I will model safe and responsible behaviour in pupils when using ICT to support learning and teaching.
- I will ensure that I am aware of my individual responsibilities relating to the safeguarding of children within the context of e-safety and know what to do in the event of misuse of technology by any member of the school community.
- I understand the importance of respecting and acknowledging copyright of materials found on the internet and will model best practice in the creation of my own resources at all times.

Agreement

I have read and understood the implications and my personal responsibilities in relation to the use of ICT equipment which is detailed within this policy.

I understand that if I fail to comply with this Acceptable Use Policy agreement, I could be subject to disciplinary action.

Name :
Role in School:
Signed
Date:
Accepted by:
Date:

Appendix 4: Video Conferencing Guidelines

Where necessary, video calling/conferencing may take place to support pupils in their learning/wellbeing. This will be done via Google Meet. The following points outline what should and should not happen if a video call takes place between staff and children:

- Only use school registered accounts, never personal ones.
- Make SLT aware of the date and time that the video call will take place.
- Ensure that, at all times, there is **more than one** school staff member present during the call.
- Ensure that the video call takes place during the working hours of school, unless otherwise approved by the Head teacher and parent/s of the child/ren.
- If there are any concerns that arise during a call about a child's safety and wellbeing, ensure that safeguarding procedures are followed.
- Parental permission does not need to be explicitly sought (if the call is taking place during school hours) however staff should remind their pupils to let an adult at home know they will be taking part.
- The call should be created as an event on our school calendar; however, children should not be directly invited via email as this gives them unmonitored access to the call. Instead, at the agreed time, a link to the Google Meet should be posted on the class' Google Classroom so that the staff are present before the children can access the livestream.
- A member of the school staff should be the last person to leave the call, thereby ending the call so children cannot re-join. The link to the call should also be taken down so children can no longer access the call.

Appendix 5: Online Safety Incident Log

ONLINE SAFETY INCIDENT LOG				
Date	**Where the incident took place**	**Description of the incident**	**Action taken**	**Name + signature of person recording the incident**