ICT ACCEPTABLE USE (E-SAFETY) POLICY

Personnel and Curriculum Committee □

Finance and Premises Committee □

Full Governing Body ☑

Christian Character Committee □

Headteacher **(Nicola Pierce)**	**Signature** N Pierce 23/05/19
Chairperson **(James Fordham)**	**Signature** J Fordham 23/05/19

Date ratified: Thursday 23rd May 2019

Review date: Summer Term 2020 (this policy will be reviewed annually)

Our Vision: To be guided by God’s wisdom, to embrace challenge and to strive to achieve our best, enjoying all that we do together.

Acceptable Use of ICT and E-safety

At St Augustine’s 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.

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 Orton St John's) who will then liaise with Updata (The Peterborough Schools Broadband network provider).

System Monitoring & Filtering

Our broadband is provided through E2BN 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, Google Apps for Education monitor all activity that occurs when the laptop/Chromebook is switched on. All access to the internet will be logged as permanent record.

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. If a student has no login, their teacher should report it to the support team for them to resolve immediately.

- 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 still and video digital cameras, for use by children and staff. . Personal devices should not be used. School provides smartphones which should be used for taking photographs and uploading to Twitter. 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 camera or smartphone as soon as possible.

Staff 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.

Email use by children

Children receive an email account on joining our school. The account will be provided by Gmail in conjunction with Google Apps for Education, which is an accredited schools provider which offers full filtering and security expected for student and staff use. The account only allows children to send and receive emails to other accounts that are in our school domain (staugustinesjunior.net). If an adult or a child has misused their email, the school can scrutinise all emails sent and received by anyone in the domain.

Mobile Phones

Children are not allowed mobile phones in school and should be handed to the school office through their class blue box for safekeeping if they are brought into school.

Internet Games

There are times in the week when children may have ‘free’ use of the school network, such as during computer clubs, 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 and sign. When using the internet children will be taught;

- How to critically evaluate materials.
- Good searching skills.

- The importance of intellectual property regarding materials they find on the internet.
- To understand how photographs can be manipulated and may attract negative attention.
- To have strategies for dealing with inappropriate materials online.
- To understand the dangers of sharing details online.

Social Networking

The use of personal Twitter, 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 twitter 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)

Appendix 2: Pupil's acceptable use agreement

Appendix 3: Staff and Volunteer Code of Conduct for ICT

Appendix 4: What to do if you see something that concerns you (E-Safety)

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.
- Close the lid of the laptop immediately and then 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. Twitter/Facebook/ Blog pages).

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: ……………………………………………

To be included in the annual safeguarding training.

APPENDIX 3: Staff or Volunteer Code of Conduct for ICT

To ensure that members of staff and volunteers at St Augustine’s Junior School are fully aware of their professional responsibilities when using information systems and when communicating with pupils, they are asked to sign this code of conduct. Members of staff and volunteers should consult the school’s Acceptable User Policy for further information and clarification.

- I understand that it is a criminal offence to use a school ICT system for a purpose not permitted by its owner.
- I appreciate that ICT includes a wide range of systems, including mobile phones, laptops/chrome books, tablets, clever touch boards, digital cameras, email and social networking.
- I understand that it is prohibited to use personal ICT devices to record or store any images of children.
- I understand that school information systems may not be used for private purposes without specific permission from the Head teacher.
- I understand that my use of school information systems, Internet and email may be monitored and recorded to ensure policy compliance.
- I will respect system security and I will not disclose any password or security information to anyone other than an authorised system manager.
- I will not install any software or hardware without permission.
- I will ensure that personal data is stored securely and is used appropriately, whether in school, taken off the school premises or accessed remotely.
- I will respect copyright and intellectual property rights.
- I will report any incidents of concern regarding children’s safety to the Designated Child Protection Coordinator or Head teacher.
- I will ensure that electronic communications with pupils only happens in the secure environment of our school learning platform and will ensure they are compatible with my professional role and that messages cannot be misunderstood or misinterpreted. The use of personal communication (in or out of school) via email, Instant Messaging and other social networking sites is prohibited.
- I will consult the head teacher regarding the appropriateness of any communication I am unsure about.
- I will promote e-safety with students in my care and will help them to develop a responsible attitude to system use, communications and publishing.

The school may exercise its right to monitor the use of the school’s information systems and Internet access, to intercept e-mail and to delete inappropriate materials where it believes unauthorised use of the school’s information system may be taking place, or the system may be being used for criminal purposes or for storing unauthorised or unlawful text, imagery or sound.

Staff or Volunteer

I acknowledge the Acceptable Use (E-Safety) Policy and the Staff or Volunteer Code of Conduct for ICT and support the school in its efforts to keep children safe when using technology and the internet as well as making them aware of the dangers.

Signed:……………………………………………… Date:……………………………

APPENDIX 4: What to do if you see something that concerns you (E-Safety Advice)

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.