Flourish Federation

E-safety and ICT acceptable use policy

This policy was ratified by Flourish Federation Governing Body on:	July 2020
This policy will be reviewed by Flourish Federation Governing Body on: (unless earlier review is required to adhere to statutory requirements/changes in procedure)	July 2022
Policy Version:	1
Policy Signed by the Chair of Governors:	*R Plant*
Policy signed by the Executive Head Teacher:	P Jones

Statement of intent 3

Legal framework 4

Use of the Internet 4

Roles and responsibilities 4

E-safety education 5

E-safety control measures 7

Reporting misuse 10

Monitoring and review 11

Appendix A 12

Appendix B 14

Appendix C 15

Appendix D 16

Appendix E **175**

Appendix F **16**

This policy has been updated in line with the requirements of the General Data Protection Regulation (GDPR), which came into effect on 25 May 2018, to include further information on consent, data security and the responsibilities of the data protection officer (DPO). The updated policy also includes reference to the 2019 version of Keeping Children Safe in Education.

Elements added or updated in response to the regulations have been highlighted as appropriate, e.g. **[New]** or **[Updated]**.

Statement of intent

At All Saints Stibbard Primary and North Elmham Primary Schools, we understand that computer technology is an essential resource for supporting teaching and learning. The Internet, and other digital and information technologies, open up opportunities for pupils and play an important role in their everyday lives.

Whilst the school recognises the importance of promoting the use of computer technology throughout the curriculum, we also understand the need for safe Internet access and appropriate use.

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.

The school is committed to providing a safe learning and teaching environment for all pupils and staff, and has implemented important controls to mitigate the risk of harm.

Signed by:

	Headteacher	Date:	
	Chair of Governors	Date:	

1. Legal framework

1.1. This policy has due regard to all relevant legislation including, but not limited to:
- The General Data Protection Regulation
- Freedom of Information Act 2000

1.2. This policy also has regard to the following statutory guidance:
- DfE (2019) 'Keeping children safe in education'
- National Cyber Security Centre (2017) 'Cyber Security: Small Business Guide'

1.3. This policy will be used in conjunction with the following school policies and procedures: (most of these policies are NCC HR policies and are therefore adopted as agreed by the Governing Body)
- Safeguarding incorporating Child Protection Policy
- Cyber Bullying Policy
- Internet, social networking and email use P319 Policy
- Allegations of Abuse Against Staff
- Data Protection

2. Use of the Internet

2.1. The school understands that using the Internet is important when raising educational standards, promoting pupil achievement and enhancing teaching and learning.

2.2. Internet use is embedded in the statutory curriculum and is therefore an entitlement for all pupils, though there are a number of controls the school is required to implement to minimise harmful risks.

2.3. When accessing the Internet, individuals are especially vulnerable to a number of risks which may be physically and emotionally harmful, including the following:
- Access to illegal, harmful or inappropriate images
- Cyber bullying
- Access to, or loss of, personal information
- Access to unsuitable online videos or games
- Loss of personal images
- Inappropriate communication with others
- Illegal downloading of files
- Exposure to explicit or harmful content, e.g. content involving radicalisation
- Plagiarism and copyright infringement
- Sharing the personal information of others without the individual's consent or knowledge

3. Roles and responsibilities

3.1. It is the responsibility of all staff to be alert to possible harm to pupils or staff due to inappropriate Internet access or use, both inside and outside of the school, and to deal with incidents of such as a priority.

3.2. The governing body is responsible for ensuring that there are appropriate filtering and monitoring systems in place to safeguard pupils.

3.3. The Headteacher is responsible for ensuring the day-to-day e-safety in the school and managing any issues that may arise.

3.4. The headteacher is responsible for ensuring that the all staff receive CPD to allow them to fulfil their role.

3.5. The Headteacher will provide all relevant training and advice for members of staff as part of the requirement for staff to undergo regularly updated safeguarding training and be able to teach pupils about online safety.

3.6. The headteacher and data protection officer (DPO) will ensure there is a system in place which monitors e-safety in the school, keeping in mind data protection requirements.

3.7. The Computing Subject lead will regularly monitor the provision of e-safety in the school and will provide feedback to the headteacher.

3.8. The headteacher will establish a procedure for reporting incidents and inappropriate Internet use, either by pupils or staff.

3.9. The Headteacher will ensure that all members of staff are aware of the procedure when reporting e-safety incidents and will keep a log of all incidents recorded.
3.10. The Headteacher will attempt to find alternatives to monitoring staff use of social media, where possible, and will justify all instances of monitoring to ensure that it is necessary and outweighs the need for privacy. The member of staff who is being monitored will be consulted prior to any interception by the school.
3.11. The governing body or safeguarding governor will meet with the Headteacher to discuss the effectiveness of the e-safety provision, current issues, and to review incident logs, as part of the school's duty of care.
3.12. The Governing Body will evaluate and review this E-safety Policy on an annual basis, considering the latest developments in ICT and the feedback from staff/pupils.
3.13. The headteacher will review and amend this policy with the DPO, taking into account new legislation, government guidance and previously reported incidents, to improve procedures.
3.14. Teachers are responsible for ensuring that e-safety issues are embedded in the curriculum and safe Internet access is promoted at all times.
3.15. All staff are responsible for ensuring they are up-to-date with current e-safety issues, and this E-safety Policy.
3.16. All staff and pupils will ensure they understand and adhere to our Acceptable Use Agreement, which they must sign and return to the headteacher.
3.17. Though school offers guidance via the school website and e-Safety cafes, parents are ultimately responsible for ensuring their child understands how to use computer technology and other digital devices appropriately when not in school.
3.18. The headteacher is responsible for communicating with parents regularly and updating them on current e-safety issues and control measures.
3.19. All pupils are aware of their responsibilities regarding the use of school-based ICT systems and equipment, including their expected behaviour.

4. E-safety education

Educating pupils:

4.1. An e-safety programme is taught across the curriculum on a regular basis, ensuring that pupils are aware of the safe use of new technology both inside and outside of the school.
4.2. Pupils will be taught about the importance of e-safety and are encouraged to be critically aware of the content they access online, including extremist material, and the validity of website content.
4.3. Pupils will be taught to acknowledge ownership of information they access online, in order to avoid copyright infringement and/or plagiarism.
4.4. Clear guidance on the rules of Internet use will be presented in all classrooms.
4.5. Pupils are instructed to report any suspicious use of the Internet and digital devices to their classroom teacher.
4.6. PSHE & Computing lessons will be used to educate pupils about cyber bullying, including how to report cyber bullying, the social effects of spending too much time online and where to access help.
4.7. The school will hold e-safety events, such as Safer Internet Day / Anti-Bullying Day to promote online safety.

Educating staff:

4.8. All staff will undergo e-safety training on at least an annual basis to ensure they are aware of current e-safety issues and any changes to the provision of e-safety, as well as current developments in social media and the Internet as a whole.
4.9. All staff will employ methods of good practice and act as role models for pupils when using the Internet and other digital devices.
4.10. All staff will be educated on which sites are deemed appropriate and inappropriate.
4.11. All staff are reminded of the importance of acknowledging information they access online, in order to avoid copyright infringement and/or plagiarism.

4.12. Any new staff are required to undergo e-safety training as part of their induction programme, ensuring they fully understand this E-safety Policy.

4.13. The Headteacher will act as the first point of contact for staff requiring e-safety advice.

Educating parents:

4.14. E-safety information will be directly delivered to parents through a variety of formats, including newsletters, the school website and e-Safety cafes.

Teaching and Learning:

4.15. This school has a clear, progressive online safety education programme as part of the computing/PSHE curriculum. This covers a range of skills and behaviours appropriate to the age of the children, including:

- To STOP and THINK before they CLICK.
- To develop a range of strategies to evaluate and verify information before accepting its accuracy.
- To know how to narrow down or refine a search / use safe search
- To understand acceptable behaviour when using an online environment/email, i.e. be polite, no bad or abusive language or other inappropriate behaviour; keeping personal information private.
- To understand why online 'friends' may not be who they say they are and to understand why they should be careful in online environments.
- To understand why they should not post or share detailed accounts of their personal lives, contact information, daily routines, location, photographs and videos and to know how to ensure they have turned-on privacy settings.
- To have strategies for dealing with receipt of inappropriate materials.
- To understand the impact of online bullying, sexting, extremism and trolling and know how to seek help if they are affected by any form of online bullying.
- To know how to report any abuse, including online bullying, and how to seek help if they experience problems when using the Internet and related technologies, i.e. parent, teacher or trusted staff member, or an organisation such as Childline or CLICK CEOP.

4.16. Teachers plan Internet use carefully to ensure that it is age-appropriate and supports the learning objectives for specific curriculum areas.

4.17. The school will remind pupils about their responsibilities through a Pupil Acceptable Use Agreement which every pupil will sign.

4.18. All staff will model safe and responsible behaviour in their own use of technology during lessons.

Online risks

4.19. The school recognises that pupils increasingly use a range of technology such as mobile phones, tablets, games consoles and computers. It will support and enable children to use these technologies for entertainment and education but will also teach children (in PSHE) that some adults and young people will use such outlets to harm children.

Cyber bullying and abuse

4.20. Cyber bullying can be defined as "Any form of bullying which takes place online or through smartphones and tablets." - BullyingUK

4.21. Complaints of online bullying are dealt with in accordance with our Anti-Bullying Policy. Complaints related to child protection are dealt with in accordance with school/LA child protection procedures.

4.22. Through the PSHE curriculum, children are taught to tell a responsible adult if they receive inappropriate, abusive or harmful emails or text messages.

4.23. Posters providing information about how to get help from Childline, ThinkUKnow and the NSPCC are displayed in classrooms and along the corridors of the school.

4.24. Cyber bullying will be treated as seriously as any other form of bullying and will be managed through our anti-bullying and confiscation procedures. Cyber bullying (along with all other

forms of bullying) of any member of the school community will not be tolerated. Full details are set out in the school's policy on anti-bullying and behaviour.

4.25. There are clear procedures in place to support anyone in the school community affected by cyberbullying.

4.26. All incidents of cyberbullying reported to the school will be recorded.

Sexual exploitation/sexting

4.27. Sexting between pupils will be managed through our anti-bullying and confiscation procedures.

4.28. All staff are made aware of the indicators of sexual exploitation and all concerns are reported immediately to the DSL.

4.29. The school will put into place to support anyone in the school community affected by sexting.

4.30. All incidents of sexting reported to the school will be recorded.

Radicalisation or extremism

4.31. Radicalisation refers to the process by which a person comes to support terrorism and forms of extremism leading to terrorism.

4.32. Extremism is defined by the Crown Prosecution Service as "The demonstration of unacceptable behaviour by using any means or medium to express views which:

- Encourage, justify or glorify terrorist violence in furtherance of beliefs.
- Seek to provoke others to terrorist acts.
- Encourage other serious criminal activity or seek to provoke others to serious criminal acts.
- Foster hatred which might lead to inter-community violence in the UK."

4.33. The school understands that here is no such thing as a "typical extremist": those who become involved in extremist actions come from a range of backgrounds and experiences, and most individuals, even those who hold radical views, do not become involved in violent extremist activity.

4.34. The school understands that pupils may become susceptible to radicalisation through a range of social, personal and environmental factors – it is known that violent extremists exploit vulnerabilities in individuals to drive a wedge between them and their families and communities. It is vital that school staff can recognise those vulnerabilities.

4.35. Staff will maintain and apply a good understanding of the relevant guidance to prevent pupils from becoming involved in terrorism.

4.36. The school will monitor its RE curriculum and assembly policy to ensure that they are used to promote community cohesion and tolerance of different faiths and beliefs.

4.37. Senior leaders will raise awareness within the school about the safeguarding processes relating to protecting pupils from radicalisation and involvement in terrorism.

5. E-safety control measures

Internet access:

5.1. All users in school are provided with usernames and passwords and will be instructed to keep these confidential to avoid any other pupils using their login details.

5.2. Effective filtering systems will be established to eradicate any potential risks to pupils through access to, or trying to access, certain websites which are harmful or use inappropriate material.

5.3. Filtering systems will be used which are relevant to pupils' age ranges, their frequency of use of ICT systems, and the proportionality of costs compared to risks.

5.4. The governing body will ensure that the use of appropriate filters and monitoring systems does not lead to 'over blocking' – unreasonable restrictions as to what pupils can be taught with regards to online teaching and safeguarding.

5.5. Any requests by staff for websites to be added or removed from the filtering list must be first authorised by the headteacher.

5.6. All school systems will be protected by up-to-date virus software.

5.7. Only portable storage which is encrypted and password protected is allowed for the storing of any personal data.
5.8. An agreed procedure will be in place for the provision of temporary users, e.g. volunteers.
5.9. Master users' passwords will be available to the headteacher for regular monitoring of activity.
5.10. Staff are able to use the Internet for personal use during out-of-school hours, as well as break and lunch times, in line with Acceptable Use policy/ Safer Working Practices
5.11. Personal use will only be monitored by the Headteacher for access to any inappropriate or explicit sites, where the need to do so outweighs the need for privacy.
5.12. Inappropriate Internet access by staff may result in the staff member being permitted to use the Internet for school purposes only and prohibited from using any personal devices. This will be dealt with following the process outlined in the misuse by staff_ section of this policy.

Email:

5.13. Pupils and staff will be given approved email accounts and are only able to use these accounts.
5.14. The use of personal email accounts to send and receive personal data or information is prohibited.
5.15. No sensitive personal data shall be sent to any other pupils, staff or third parties via email.
5.16. Pupils are made aware that all email messages are monitored and that the filtering system will detect inappropriate links, viruses, malware and profanity.
5.17. Staff members are aware that their email messages are monitored.
5.18. Any emails sent by pupils to external organisations will be overseen by their class teacher and must be authorised before sending.
5.19. Chain letters, spam and all other emails from unknown sources will be deleted without opening.
5.20. As part of their teaching, class teachers will inform their pupils what a phishing email might look like – this will include information on the following:
- Determining whether or not an email address is legitimate
- Knowing the types of address a phishing email could use
- Asking "does it urge the recipient to act immediately?"
- Checking the spelling and grammar

5.21. Staff will not be punished if they are caught out by cyber-attacks as this may prevent similar reports in the future. The Headteacher will conduct an investigation; however, this will be to identify the cause of the attack, any compromised data and if there are any steps that can be taken in the future to prevent similar attacks happening.

Social networking:

5.22. The use of social media on behalf of the school will be conducted following the processes outlined in our Internet, social networking and media use policy.
5.23. Access to social networking sites will be filtered as appropriate.
5.24. Should access be needed to social networking sites for any reason, this will be monitored and controlled by staff at all times and must be first authorised by the headteacher.
5.25. Pupils and parents will be advised that the use of social network spaces bring a range of dangers for primary aged pupils.
5.26. ~~Pupils will be advised to use~~ nicknames and avatars ~~when using social networking sites~~
5.27. Pupils are regularly educated on the implications of posting personal data online outside of the school.
5.28. Staff will be advised to "block" their profile picture from being downloaded and protect their profile information.
5.29. Staff are regularly educated on posting inappropriate photos or information online, which may potentially affect their position and the school as a whole.
5.30. Staff are not permitted to communicate with pupils over social networking sites and are reminded to alter their privacy settings.

5.31. Staff are not permitted to publish comments about the school or include comments about school activities without discussing it with the headteacher first.
5.32. Staff are not permitted to access social media sites during teaching hours unless it is beneficial to the material being taught. This will be discussed with the headteacher prior to accessing the social media site.

Published content on the school website:

5.33. The computing lead will be responsible for the overall content of the website and will ensure the content is appropriate and accurate.
5.34. Contact details on the school website will include the phone number, email and address of the school – no personal details of staff or pupils will be published.
5.35. Images, video and sound recordings of pupils will only be used in school publications and the school website with parental consent.
5.36. Only first names of children will be used in school publications or the website.
5.37. Staff are able to take pictures, though they must do so in accordance with our Photography Policy. Staff will not take pictures using their personal equipment.
5.38. Any member of staff that is representing the school online, e.g. through blogging, must express neutral opinions and not disclose any confidential information regarding the school, or any information that may affect its reputability.

Mobile devices and hand-held computers:

5.39. Mobile devices are not permitted to be used during school hours by pupils
5.40. Staff may only use mobile devices in their break and lunchtimes away from classrooms and after school hours
5.41. The sending of inappropriate messages or images from mobile devices is prohibited.
5.42. Only school provided Mobile devices will be used to take images, videos or sound recordings of pupils or staff.
5.43. A safeguarding concern may be triggered if school has reasonable suspicion that a member of staff has inappropriate material on a mobile device on the school premises resulting in the police being informed.
5.44. The Headteacher will, in collaboration with the ICT technician, ensure all school-owned devices are password protected.
5.45. Tracking software will be activated on mobile devices to enable retrieval if lost or stolen.
5.46. Headteacher will review all mobile devices and hand-held computers to ensure all apps are compliant with data protection regulations and up-to-date, and to carry out any required updates.
5.47. The Headteacher will review and authorise any apps and/or computer programmes before they are downloaded.
5.48. Apps will only be downloaded from manufacturer approved stores, e.g. Google Play and the Apple App Store and with the prior consent of the Headteacher

Network security:

5.49. All staff and children accessing Chromebooks can only do so with their own personal account.
5.50. Passwords have a minimum and maximum length, to prevent 'easy' passwords or mistakes when creating passwords.
5.51. Passwords will require a mixture of letters, numbers and symbols to ensure they are secure as possible.
5.52. Passwords should be reset every term to ensure security
5.53. Passwords should be stored using non-reversible encryption.
5.54. The following passwords will not be accepted by the school's security systems as they are too predictable:
- Password
- Pa55word
- Password123

- Qwerty
- 123456
- 12345678
- ABC123

5.55. The Headteacher and ICT technician will ensure all school-owned laptops and computers have their encryption settings turned on where appropriate or, if there is no built-in encryption option, encryption software is installed.

Virus management:

5.56. Technical security features, such as virus software, are kept up-to-date and managed by the Headteacher.

5.57. The ICT Technician will ensure that the filtering of websites and downloads is up-to-date and monitored.

5.58. Firewalls will be switched on at all times – ICT technicians will review these on a fortnightly basis to ensure they are running correctly and to carry out any required updates.

5.59. Firewalls and other virus management systems, e.g. anti-virus software, will be maintained in accordance with the school's policies

5.60. Staff members will report all malware and virus attacks to the Headteacher and DPO immediately.

E-safety committee:

5.61. The E-safety Policy will be monitored and evaluated by the designated Safeguarding Governor on an annual basis.

Use of CPOMS:

5.62. All staff have a duty to record safeguarding concerns onto the CPOMS website using their own school email address login (with the use of the 'pink' safeguarding forms discontinuing).

5.63. Should staff require second level authentication then another school device is preferred for this app to be downloaded on (i.e. a tablet) over a personal mobile phone. Should staff require to use their personal mobile phone for second level authentication in school hours then this should be done in the school office.

6. Reporting misuse

6.1. All Saints CEVA Primary School, Stibbard and North Elmham CEVC Primary School will clearly define what is classed as inappropriate behaviour in the Acceptable Use Agreement, ensuring all pupils and staff members are aware of what behaviour is expected of them.

6.2. Inappropriate activities are discussed and the reasoning behind prohibiting activities due to e-safety are explained to pupils as part of the curriculum in order to promote responsible Internet use.

Misuse by pupils:

6.3. Teachers have the power to discipline pupils who engage in misbehaviour with regards to Internet use.

6.4. Any instances of misuse should be dealt with in line with our behaviour policy, be immediately reported to a member of staff and recorded on the behaviour log. Appropriate sanctions may be used including being referred to the headteacher.

6.5. Any pupil who does not adhere to the rules outlined in our Acceptable Use Agreement and is found to be wilfully misusing the Internet will have a letter sent to their parents explaining the reason for suspending their Internet use.

6.6. Complaints of a child protection nature, such as when a pupil is found to be accessing extremist material, shall be dealt with in accordance with our Child Protection and Safeguarding Policy.

Misuse by staff:

6.7. Any misuse of the Internet by a member of staff should be immediately reported to the headteacher.
6.8. The headteacher will deal with such incidents in accordance with the Allegations of Abuse Against Staff and this may result in take disciplinary action against the member of staff.
6.9. The headteacher will decide whether it is appropriate to notify the police or the LADO of the action taken against a member of staff.

Use of illegal material:

6.10. In the event that illegal material is found on the school's network, or evidence suggests that illegal material has been accessed, the police will be contacted.
6.11. Incidents will be immediately reported to the Internet Watch Foundation and the police will be contacted if the illegal material is, or is suspected to be, a child sexual abuse image hosted anywhere in the world, a non-photographic child sexual abuse image hosted in the UK, or criminally obscene adult content hosted in the UK.
6.12. If a child protection incident is suspected, the school's child protection procedure will be followed – the DSL / headteacher will be informed and the police contacted.
6.13. Staff will not view or forward illegal images of a child. If they are made aware of such an image, they will contact the DSL.

7. Monitoring and review

7.1. The Governing Body will evaluate and review this E-safety Policy on three year basis, taking into account the school's e-safety calendar, the latest developments in ICT and feedback from staff/pupils.
7.2. Members of staff are required to familiarise themselves with this policy as part of their induction programmes.

Appendix A

Staff, Governor and Visitor Acceptable Use Agreement

ICT and the related technologies, such as email, the Internet and mobile devices, are an expected part of daily working life in school. This policy is to help ensure that all staff are aware of their professional responsibilities when using any form of ICT and to help keep staff, governors and visitors safe. All staff are expected to sign this agreement confirming their undertaking to adhere to its contents at all times. Any concerns or clarification should be discussed with the headteacher.

- I will only use the school's email, Internet, learning platform and hand held devices and any related technologies for professional purposes or for uses deemed 'reasonable' by the headteacher or governing body.
- I understand it is an offence to use the ICT system and equipment for any other purpose not permitted by its owner (i.e. the school)
- I will comply with the ICT system security and not disclose any passwords provided to me by the school or other related authorities.
- I will ensure that all electronic communications with pupils and staff are compatible with my professional role.
- I will not give out my personal details, such as mobile phone number or personal email address, to pupils.
- I will only use the approved email system for any communications with pupils, parents and other school-related activities.
- Images will only be taken in line with this policy and with the consent of parents and individuals (in the case of staff)
- I understand that I will follow the schools Clear Screen Policy and never leave a workstation unattended and logged on.
- Any equipment used, such as laptops, must be signed for off-site and responsibility for the equipment remains with the member of staff. This policy remains valid whilst it is not on the school's premises.
- Any equipment left on the premises overnight must be in a secure, alarmed area.
- I will ensure that personal data (such as data held on the administration system) is kept secure and is used appropriately. Personal data can only be taken out of the school or accessed remotely when authorised by the headteacher or governing body and with appropriate levels of security in place.
- I will not install any hardware or software on school equipment without the permission of the headteacher.
- I will report any accidental access to inappropriate materials immediately to my line manager.
- I will not browse, download, upload or distribute any material that could be considered offensive, illegal or discriminatory.
- Images of pupils and/or staff will only be taken, stored and used for professional purposes in line with data protection policy and with written consent of the parent or staff member. Images will not be distributed outside the school network without the permission of the parent, member of staff or headteacher in line with data security procedures
- I understand that all my use of the Internet and other related technologies can be monitored and logged and can be made available to the headteacher. Including on my own mobile devices.
- I will respect copyright and intellectual property rights.
- I will ensure that my online activity, both in school and outside school, will not bring my professional role into disrepute. This includes ignoring invitations from pupils and parents to be part of their social networking site(s).
- I will support and promote the school's E-safety Policy and help pupils to be safe and responsible in their use of ICT and related technologies.

User signature

I agree to follow this acceptable use policy and to support the safe use of ICT throughout the school. I understand that violation of this policy may be subject to disciplinary action, up to and including termination of employment and the instigation of criminal proceedings

Signature _____

Date _____

Full name _____ (Printed)

Appendix B

Acceptable Use Agreement: Pupils

Class: _____

Year: _____

Pupil Acceptable Use Agreement

- I will only use ICT in school for school purposes.
- I accept that I am responsible for all activity carried out under my username
- I will only use my own school email address when emailing.
- I will only open email attachments from people I know, or who my teacher has approved.
- I will not tell other people my passwords.
- I will only open/delete my own files or documents shared through Google Drive/Classroom by teachers or my classmates.
- I will make sure that all ICT related contact with other children and adults is appropriate, responsible, respectful and polite.
- I will be responsible for my behavior when using the Internet.
- I will not deliberately look for, save or send anything that could offend others.
- If I accidentally find anything inappropriate on the Internet I will tell my teacher immediately.
- I will not give out my personal details such as my name, phone number, home address or school.
- I will be responsible for my behaviour when using ICT in school or at home because I know that these rules are to keep me safe.
- I will not arrange to meet someone unless this is part of a school project approved by my teacher and a responsible adult comes with me.
- I know that my use of ICT can be checked and that my parent contacted if a member of school staff is concerned about my safety.
- I understand that these rules are to keep me safe and that I can only use the schools equipment if I follow the rules.
- I will not bring a mobile phone or other personal ICT device into school.
- I will not take photographs or film using a mobile phone

Signature pupil: _____

Signature parent: _____

Date: _____

Appendix C

Acceptable Use Agreement: Parents

Parent's/Carer's name: _____ **(PLEASE PRINT)**
Child's name: _____ **Year and Class:** _____
Child's name: _____ **Year and Class:** _____
Child's name: _____ **Year and Class:** _____

- I know that my child(ren) has/have signed a form to confirm that they will keep to the school's rules for responsible ICT use, outlined in the e-Safety and ICT Acceptable Use Rules for Children. I also understand that my son/daughter may be informed, if the rules have to be changed during the year. I know that the latest copy of the e-Safety and ICT Acceptable Use Policy and the Rules are available on the school's website
- I accept that ultimately the school cannot be held responsible for the nature and content of materials accessed through the Internet and mobile technologies, but I understand that the school will take every reasonable precaution to keep children safe and to prevent children from accessing inappropriate materials. These steps include using a filtered Internet service, secure access to email, employing appropriate teaching practice and teaching e-Safety skills to children.
- I understand that the school can check my child's computer files, and the Internet sites they visit. I also know that the school may contact me if there are concerns about my son/daughter's e-Safety or e-behaviour.
- I will support the school by promoting safe use of the Internet and digital technology at home and will inform the school if I have any concerns over my child's e-Safety.

Parent's signature: _____ Date: _____

Appendix D

Rules for EYFS and KS1

Think then Click

These rules help us to stay safe on the Internet

E-safety rules for EYFS and KS1

- ✓ We only use the Internet when an adult is with us.
- ✓ We can click on the buttons or links when we know what they do or where they take us.
- ✓ We can use the Internet to search for things when an adult is with us.
- ✓ We always stop and ask for help if we get lost on the Internet.
- ✓ We can send and open emails with a grown-up.
- ✓ We can write polite and friendly emails to people we know.
- ✓ We never share our names or addresses on the Internet.
- ✓ We know that friends are people we know in the real world not people we meet online.




Appendix E

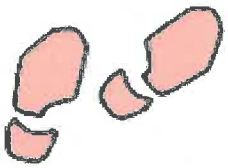
Rules for KS2

Think then Click

These rules help us to stay safe on the Internet

E-safety rules for KS2

- ✓ We ask permission before using the Internet.
- ✓ We only look at websites an adult has given us permission to use.
- ✓ We always tell an adult if we have seen, heard or read anything on the Internet that has made us feel threatened, uncomfortable or worried.
- ✓ We immediately close a web page if we are unsure.
- ✓ We only send polite and friendly emails to people we know or that an adult has approved.
- ✓ We never give out personal information or passwords.
- ✓ We never arrange to meet anyone we don't know.
- ✓ We do not open emails sent by anyone we don't know.
- ✓ We do not use Internet chat rooms.
- ✓ We know that friends are people we know in the real world not people we meet online.




Appendix F

Additions to E safety policy and ICT Acceptable Use during coronavirus time June 15th 2020, to include reflections of working online directly with students~:

- Linked to Remote Learning policy
- All staff to use their work/school email address for transparency and for checking (Never use personal email accounts).
- All staff to ensure parents consent to the online/virtual communication by completing the agreed Flourish Federation proforma - sent to parents via email from the office.
- All online teaching/working remotely must happen during school hours to ensure professional distance expected from our staff, to protect pupils family time and to safeguard workload.
- All online teaching/working remotely to include another school teaching practitioner presence (teachers / teaching assistant) to ensure safer working practice and for this to take place after bubble time in the afternoons. Or, when working from home, two teaching practitioners are to be present in the meeting.
- All practitioners engage in professional curiosity as set out in the Code of Conduct when working online directly with students and from home learning experiences. To record any observations/issues/concerns on CPOMs to alert DSL's as you would in a school environment.
- All teaching staff acknowledge that our offer of 'blended learning approach' during this coronavirus time delivers that which is agreed by SLT and that nothing is delivered above and beyond which has not been shared and agreed by SLT in advance and or the Governing body if appropriate for amendment to coronavirus risk assessment.
- No recording of Zoom/Google Meet and other virtual meeting platforms.
- Any Zoom /Google Meet or other virtual meeting platforms to have a minimum of 3 pupils present.
- When using any Zoom /Google Meet or other virtual meeting platforms, staff to be aware of their physical background, be dressed appropriately, alert family members that a meeting is taking place beforehand to maintain professionalism and that no family members join the meet nor allow any parent to interrupt the meet. Where a parent wishes to interrupt, pause the lesson and state you will contact them after the meeting.
- Teacher to end the virtual meeting so all leavers close.
- Practitioners to use Tapestry during coronavirus times as you would during school times for sharing and uploading wow moments / comments for pupil's learning profiles.