Be the best for God you can be!

Our vision is that we become the best for God that we can be, in all we do, whilst demonstrating Christian values which are pertinent to all faiths.

Our vision is based on Colossians 3:23. *'Whatever you do, work at it with all your heart, as though you were working for the Lord and not for people.'*

Trust:
'Trust in the Lord with all your heart and lean not on your own understanding'
Proverbs 3:5

Compassion:
'Love the Lord your God with all your heart, with all your soul and with all your mind. And love your neighbour as yourself'
Matthew 22:37

Thankfulness:
'Be thankful in all circumstances. This is what God wants from you in your life'
Thessalonians 5:18

Hope:
'But those who hope in the Lord will renew their strength'
Isaiah 40:31

Perseverance:
'I know your deeds, your love and faith, your service and perseverance'
Revelations 2:19

Forgiveness:
'For if you forgive other people when they sin against you, your heavenly father will also forgive you'
Matthew 6:14

Online Safety Policy

1. Writing and Reviewing the Online Safety Policy

The Online Safety Policy relates to other policies including those for ICT Security, Remote Learning, Antibullying and Safeguarding and Child Protection.

- Ismail Rawat is the school's Online Safety Co-ordinator who will work in collaboration with Jennifer Cunningham (Safeguarding & DSL) and Debbie Withey (Headteacher).
- Our Online Safety Policy has been written by the school, building on guidance from Blackburn with Darwen Council and government guidance. It has been agreed by staff and approved by governors.
- The Online Safety Policy and its implementation will be reviewed annually or in response to an incident using the attached audit (Appendix 4).
- As schools increasingly work online, it is essential that children are safeguarded from potentially harmful and inappropriate online material. As such, the Governing Body ensures that appropriate filters and monitoring systems are in place. At St Barnabas and St Paul's, we use the Lightspeed monitoring system provided by Blackburn Council.
- In order to ensure that our Online Safety provision is current and effective, the Governing Body will carry out an annual self-review of the school's online safety provision using the CSAP Online Safety Governance Self-Review Tool.

2. Teaching and Learning

As the children's access and understanding expands, so should the guidance and rules to ensure safe access use of the internet.

It is essential that children are safeguarded from potentially harmful and inappropriate online material. Our approach to online safety empowers pupils, students, and staff in their use of technology and establishes mechanisms to identify, intervene in, and escalate any concerns where appropriate.

The breadth of issues classified within online safety is considerable, but can be categorised into four areas of risk:

- content: being exposed to illegal, inappropriate or harmful content, for example:
  pornography, fake news, racism, misogyny, self-harm, suicide, anti-Semitism, radicalisation and extremism.
- contact: being subjected to harmful online interaction with other users; for example: peer to peer pressure, commercial advertising and adults posing as children or young adults with the intention to groom or exploit them for sexual, criminal, financial or other purposes'.
- conduct: personal online behaviour that increases the likelihood of, or causes, harm; for example, making, sending and receiving explicit images (e.g consensual and non-consensual sharing of nudes and semi-nudes and/or pornography, sharing other explicit images and online bullying; and
- commerce - risks such as online gambling, inappropriate advertising, phishing and or financial scams. If you feel your pupils, students or staff are at risk, please report it to the Anti-Phishing Working Group (https://apwg.org/).

Why Internet use is important?

Internet use is part of the curriculum and a necessary tool for learning, which is widely used at St Barnabas and St Paul's. The internet is a part of everyday life for education, business and social interaction. The school has a duty to provide students with quality Internet access as part of their learning experience.

- The purpose of internet use in school is to raise educational standards, to promote pupil achievement, to support the professional work of staff and to enhance the school's management functions.
- Internet access is an entitlement for students who show a responsible and mature approach to its use.
- Internet use is a part of the statutory curriculum and a necessary tool for staff and pupils.

How does the internet use benefit education?

Benefits of using the internet in education include:

- Access to worldwide educational resources including museums and art galleries;
- Educational and cultural exchanges between pupils locally, nationally and worldwide;
- Vocational, social and leisure use in libraries, clubs and at home;
- Access to experts in many fields for pupils and staff;
- Professional development for staff through access to national developments, associations;
- Improved access to technical support including remote management of networks and automatic system updates;
- Access to learning wherever and whenever convenient.
- Educational materials and effective curriculum practice;
- Collaboration across networks of schools, support services and professional.

Pupils will be taught how to evaluate internet content appropriate to their age.

Many of our pupils use the internet widely outside of school and need to learn how to evaluate internet information and to take care of their own safety and security.

- Pupils will be taught what internet use is deemed as responsible and what is not and given clear objectives for internet use.
- Pupils will be educated in the effective use of the internet in research, including the skills of knowledge location, retrieval and evaluation appropriate to their age group.
- Sanctions for inappropriate use of the internet will be explained to the children.
- Pupils should be taught to be critically aware of the materials they read and shown how to validate information before accepting its accuracy.
- The school will ensure that the use of internet derived materials by staff and pupils complies with copyright law.

3. Managing Internet Access

Information System Security

- School ICT systems capacity and security will be reviewed regularly by the LA and Headteacher/ICT support.
- Virus protection is updated regularly.
- Security strategies will be discussed with Blackburn with Darwen LA and ICT support.

Managing Filtering

- The school will work with the LA, DfE and the Internet Service Provider to ensure systems to protect pupils are reviewed and improved.
- If staff or pupils discover an unsuitable site, it must be reported to the Internet Safety Coordinator and the LA will be informed so that they can take appropriate action.

- Regular checks are made by the DSL and online safety co-ordinator to ascertain the robustness of the filtering. A filtering software checklist is completed and shared with the Headteacher. Any areas of concern are addressed immediately with BwD.
- The school uses the **Lightspeed** system to monitor internet usage in school on a weekly basis.

How email will be managed

Staff should use only their designated school email address, rather than personal email, for all professional purposes. Children cannot access personal email or social networking sites such as Facebook within school.

4. Staying Safe

The school will ensure pupils and parents are aware of and adhere to the school's Online Safety Rules – Pupil User Agreements (Appendix 1).

- The school internet access is designed expressly for pupil use and includes appropriate filtering.
- Pupils may only use approved digital methods of communication on the school system e.g. not forwarding chain letters.
- Pupils will be taught to tell an adult immediately about any offensive communications they receive or any inappropriate content they may encounter using digital technology.
- Pupils and staff will use equipment responsibly.
- Pupils will be advised never to give out personal details of any kind which may identify them or their location or arrange to meet anyone without specific permission.
- Pupils and parents will be advised that the unsupervised use of social network spaces outside school is inappropriate for pupils.

Published Content:

- Any information that can be accessed outside the school's intranet should be classed as published whether in electronic or paper format.
- Electronic communication sent to an external organisation should be written carefully and authorised before sending, in the same way as a letter written on school headed paper.
- General contact details should be the school address, email and telephone number. Staff or pupils' personal (excluding full name for pupils) information will not be published.
- The Headteacher will take overall editorial responsibility and ensure that content is accurate and appropriate.

Publishing pupil's images and work:

- Staff and pupils using iPads, cameras, video recorders or sound recorders will ensure that they inform others before recording on them & always use equipment in a respectful manner as stated in the Online Safety Rules and Pupil User Agreement (Appendix 1).
- Only appropriate photographs are to be published online.
- Pupils' full names will not be used anywhere online, particularly in association with photographs.
- Written permission must be provided for children's work, photos and videos to be taken and published online. This is obtained through the general parental consent form.
- Parents and children will be asked to sign an Online Safety Rules – Pupil User Agreement when starting school & again when entering a new key stage/phase. Copies of the agreement may be sent home at the start of the year or during Safety Week to remind pupils & parents.

Managing emerging technologies:

- The educational benefit of emerging technologies and any potential risks will be considered before it is used in school. Children are not permitted to have or use mobile phones in school.

Protecting personal data

- Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 2018.

How online bullying (also referred to as cyber bullying) will be managed:

The rapid development of, and widespread access to technology has provided a new medium for 'virtual' bullying, which can occur in or outside school. Cyber-bullying is a form of bullying and can happen at all times of the day, with a potentially bigger audience, and more accessories as people forward on content at a click. Online / cyber bullying can occur via mobile phones or online (e.g. text messaging (including sexting), emailing, videoing, social networks, gaming, instant messenger etc.

Many young people and adults find using the internet through various means a positive and creative part of their every day. Unfortunately, technologies can also be used negatively. All staff and pupils in school are aware of how online / cyber bullying is different from other forms of bullying and how it can affect people.

Online / cyber bullying (along with all forms of bullying) will not be tolerated in school. Full details are set out in the school's Anti-bullying Policy.

There are clear procedures in place to support anyone affected by online bullying:

- All incidents of cyber bullying reported to school will be recorded using our reporting system CPOMS.
- Clear procedures are in place to investigate incidents or allegations of online bullying.
- The school will take steps to identify the person/s responsible for the bullying.
- Contact parents/carers when necessary.
- To take any appropriate disciplinary action.
- Sanctions for those involved in online bullying may include - internet access may be suspended for a period of time, parents/carers may be informed, and the police will be contacted if a criminal offence is suspected.

5. Policy Decisions

Authorising Internet Access:

- All staff must read and sign the school's Online Safety Policy and ICT Security & Acceptable Use Policy and User Agreement before using any school ICT resource (Appendix 2).
- Staff will be reminded of the agreement every September when we share our Staff Handbook. New staff will receive the information through the school's induction procedures.
- The school will keep a record of all staff and pupils who are granted internet access. The record will be kept up-to-date, for instance a member of staff may leave or a pupil's access be withdrawn. This will be stored centrally by the School Operations Manager.
- Parents and pupils will be asked to sign and return the school's 'Online Safety Rules and Pupil User Agreement (Appendix 1).

Assessing Risks

- The school will take all reasonable precautions to ensure that users access only appropriate material. However, due to the international scale and linked nature of internet content, it is not possible to

guarantee that unsuitable material will never appear on a school computer. Neither the school nor Blackburn with Darwen LA can accept liability for the material accessed, or any consequences of internet access. Any inappropriate access whether intentional or unintentional will be reported to the Online Safety Co-ordinator (Ismail Rawat) who will report to the Headteacher and DSL, and to Blackburn Council where necessary.

- The school will audit ICT provision to establish if the Online Safety Policy is adequate and that its implementation is effective.

Handling Online Safety Complaints

- Complaints of internet misuse will be dealt with by the Headteacher or another a senior member of staff alongside the DSL, and where appropriate they will inform Blackburn Council.
- Any complaint about staff misuse must be referred to the Headteacher.
- Complaints of a child protection nature must be dealt with in accordance with school's child protection policy and procedures.
- Pupils and parents will be informed of the complaints policy and procedure on request. This is also available to view on the school's website https://www.stbarnabas-stpauls.co.uk/

6. Communication of Policy & Procedures

Introducing the Online Safety Policy to pupils

- Online Safety Rules will be posted in all networked rooms and classrooms and discussed and shared with the pupils at the start of each year.
- Pupils are asked to sign an Online Safety Rules/Agreement when starting school or when entering a new key stage/phase.
- Pupils will be informed that network and internet use will be monitored and can be monitored and traced to the individual device or login.
- Pupils will be taught aspects of online safety through the computing curriculum e.g. how to search safely, what information can be shared when working on email.
- All pupils will take part in internet safety activities during the school's annual Safety Week. Online Safety will be taught using the 'Think you know' resources provided by the Child Exploitation and Online Protection agency (CEOP).

Staff and the Online Safety Policy

- All staff will be provided with a copy of the school's Online Safety Policy and its importance explained.
- Staff will read through the Online Safety Guidance (appendix 3) and use for online safety support.
- Staff should be aware that internet traffic may be monitored and traced to the individual device or login. Discretion and professional conduct is essential.
- The school may use monitoring software where this is available to ensure that inappropriate materials are not being stored or used on school equipment.

Enlisting Parents/Carers Support

- Parents/carers attention will be drawn to the school's Online Safety Policy and support available in newsletters and on the school's website under Key Information – Safeguarding & Child Protection - Online Safety https://www.stbarnabas-stpauls.co.uk/safeguarding-and-child-protection/Links to guidance and websites offering support for parents will be provided on our school website.

Review date: Spring 2024

Appendix 1 – Pupil and Parent Online Safety Rules & User Agreement

St Barnabas and St Paul's CE Primary School

Online Safety Agreement 2021-22

As part of the National Curriculum, all pupils use technology including the internet and communication technology in their learning. Both pupils and parents/carers are asked to sign to show that the Online Safety Rules on the reverse of this agreement have been understood and agreed. Children will sign a class agreement every year with their teacher in class.

Pupil Agreement

Early Years and Key Stage 1

- I only use the internet when an adult is with me
- I only click on links and buttons online when I know what they do
- I keep my personal information and passwords safe
- I only send messages online which are polite and friendly
- I know the school can see what I am doing online
- I use the iPads for what I have been asked and I use my allocated iPad
- I always tell an adult if something online makes me feel unhappy or worried
- I have read and talked about these rules with my parents/carers

Key Stage 2

Safe

- I send messages which are polite and friendly
- I post pictures or videos on the internet if they are appropriate, and if I have permission
- I talk with and open messages from people I know, and I only click on links if I know they are safe
- I talk to an adult if somebody says something that makes me feel uncomfortable online

Trust

- I will check content on other sources like other websites, books or with a trusted adult
- I always credit the person or source that created any work, image or text I use

Responsible

- I always ask permission from an adult before using the internet
- I only use websites that my teacher has recommended and I use SafeSearch as a search engine
- I use the iPads for what I have been asked and I use my allocated iPad

- I use school computers for school work, unless I have permission otherwise
- I keep my personal information safe and private online
- I will keep my passwords safe and not share them with anyone
- I will not access or change other people's files or information
- I will not bring my own personal devices to school
- I will only change the settings on the computer if a teacher has allowed me to.

Understand

- I understand that the school internet filter is there to protect me, and I will not try to bypass it
- I know that my use of school devices/computers and internet access will be monitored
- I have read and talked about these rules with my parents/carers
- I can visit www.thinkuknow.co.uk and www.childline.org.uk to learn more about being safe online.

Tell

- If I am aware of anyone being unsafe with technology, I will report it to a teacher or other adult
- I always talk to an adult if I'm not sure about something or if something happens online that makes me feel worried or frightened
- If I see anything online that I shouldn't or that makes me feel worried or upset, then I will tell an adult straight away.

St Barnabas and St Paul's CE Primary School Acceptable Use of Technology Policy – Pupil Agreement

I, with my parents/carers, have read and understood the St Barnabas and St Paul's Acceptable Use of Technology Policy (AUP).

I agree to follow the AUP when

1. I use St Barnabas and St Paul's systems and devices, both on and offsite

2. I use my own equipment outside school, in a way that is related to me being a member of the St Barnabas and St Paul's community, including communicating with other members of the school.

Name……. Signed…….

Class…… Date…….

Pupils in KS2 should sign this agreement themselves; parents of children in KS1 may sign it on their behalf once the information has been discussed.

Parent/Carer Agreement - Internet Access and Related Technologies

Videos and Photographs

Children may be photographed and these images used for assessment to record learning or to help children present ideas. Images and videos of pupils will not be published on the school's website or online without permission.

- I, with my child, have read and discussed St Barnabas and St Paul's pupil acceptable use of technology policy (AUP). I understand that the aim of the AUP is to help keep my child safe online and applies to the use of the internet and other related devices and services, inside and outside of the school.

- I am aware that any internet and IT use using school equipment may be monitored for safety and security reason to safeguard both my child and the school systems. This monitoring will be proportionate and will take place in accordance with data protection, privacy and human rights legislation.

- I understand that the school will take every reasonable precaution, including monitoring and filtering systems, to ensure my child will be safe when they use the internet and other associated technologies.

I understand that the school cannot ultimately be held responsible for the nature and content of materials accessed on the internet and using mobile technologies.

- I will support school safeguarding policies and will ensure that I appropriately monitor my child's use of the internet outside of school and discuss online safety with them when they access technology at home.

- I, with my child, am aware of the importance of safe online behaviour and will not deliberately upload or add any images, video, sounds or text that could upset, threaten the safety of or offend any member of the school community.

- I understand that the school will contact me if they have concerns about any possible breaches of the AUP or have any concerns about my child's safety.

- I will inform the school or other relevant organisations if I have concerns over my child's or other members of the school community's safety online.

- I know that my child will receive online safety education to help them understand the importance of safe use of technology and the internet – both in and out of school.

- I will support the school online safety approaches and will encourage my child to adopt safe use of the internet and other technology at home, as appropriate to their age and understanding. I know that I can speak to the Designated Safeguarding Lead (Jennifer Cunningham), my child's teacher or the Head teacher, if I have any concerns about online safety.

I have read the school's Acceptable Use of Technology policy and agree to support the school in keeping my child safe online.

Child's Name…….. Class……

Parents Name……

Parents Signature……

Date…….



Appendix 2 – Staff ICT Security & Acceptable Use Agreement

To ensure that staff are fully aware of their professional responsibilities when using information systems, they are asked to sign this code of conduct. Staff should consult the school's ICT Security & Acceptable Use Policy and Online Safety Policy for further information and clarification. Copies of these will be provided to all staff every September and available on the shared drive – Staff Shared - Policies. This includes guidance for staff on the use of social networking sites.

1. I understand that this AUP applies to my use of technology systems and services provided to me or accessed as part of my role within St Barnabas and St Paul's both professionally and personally. This may include use of laptops, mobile phones, tablets, digital cameras and email as well as IT networks, data and data storage and online and offline communication technologies.

2. I understand that the Acceptable Use of Technology Policy (AUP) should be read and followed in line with the school's code of conduct.

3. I am aware that this AUP does not provide an exhaustive list; all staff should ensure that technology use is consistent with the school ethos, staff behaviour and safeguarding policies, national and local education and child protection guidance, and the law.

Use of School Devices and Systems

4. I will only use the equipment and internet services provided to me by the school (for example, school provided laptops, tablets, mobile phones and internet access) when working with children, unless I have permission from the Head teacher.

5. I understand that any equipment and internet services provided by my workplace is intended for educational use and should only be accessed by members of staff.

6. Only school/setting issued devices will be used for apps that record and store children's personal details, attainment or photographs. Personal staff mobile phones or devices will not be used to access or upload content to any apps which record and store children's personal details, attainment or images. Such information should be accessed or uploaded at school.

Data and System Security

7. To prevent unauthorised access to systems or personal data, I will not leave any information system unattended without first logging out or securing/locking access.

8. I will use a 'strong' password to access school systems. A strong password has numbers, letters and symbols, with 8 or more characters and does not contain a dictionary word.

9. I will protect the devices in my care from unapproved access or theft by ensuring they are not left visible or unsupervised in public places.

10. I will respect school system security and will not disclose my password or security information to others.

11. I will not open any hyperlinks or attachments in emails unless they are from a known and trusted source. If I have any concerns about email content sent to me, I will report them to the IT system manager.

12. I will not attempt to install any personally purchased or downloaded software, including browser toolbars, or hardware without permission from the IT system manager.

13. I will ensure that any personal data is kept in accordance with the Data Protection legislation, including GDPR in line with the school information security policies.

- All personal data will be obtained and processed fairly and lawfully, only kept for specific purposes, held no longer than necessary and will be kept private and secure with appropriate security measures in place, whether used in the workplace, hosted online or accessed remotely.
- Any data being removed from the school site, such as via email or on memory sticks or CDs, will be suitably protected. All memory sticks used must be encrypted.

14. I will not keep documents which contain school related sensitive or personal information, including images, files, videos and emails, on any personal laptops, digital cameras, and mobile phones. However, I may access the school email via my mobile phone outside school.

15. I will not store any personal information on the school IT system, including school laptops or similar device issued to members of staff, that is unrelated to school activities, such as personal photographs, files or financial information.

16. I will ensure that school owned information systems are used lawfully and appropriately. I understand that the Computer Misuse Act 1990 makes the following criminal offences: to gain unauthorised access to computer material; to gain unauthorised access to computer material with intent to commit or facilitate commission of further offences or to modify computer material without authorisation.

17. I will not attempt to bypass any filtering and/or security systems put in place by the school.

18. If I suspect a computer or system has been damaged or affected by a virus or other malware, I will report this to the ICT Support Provider (BlueOrange) as soon as possible.

19. If I have lost any school related documents or files, I will report this to the ICT Support Provider (BlueOrange) and School Data Protection Officer (Angela Brennan) as soon as possible.

20. Any images or videos of pupils will only be used as stated in the school image use policy:

- I understand images of pupils must always be appropriate and should only be taken with school provided equipment and taken/published where pupils and their parent/carer have given explicit consent.

Classroom Practice

21. I am aware of safe technology use in the classroom and other working spaces, including appropriate supervision of pupils, as outlined in the school online safety policy.

22. I have read and understood the school online safety policy which covers expectations for pupils regarding mobile technology and social media.

23. I will promote online safety with the pupils in my care and will help them to develop a responsible attitude to safety online, system use and to the content they access or create by:

- exploring online safety principles as part of an embedded and progressive curriculum and reinforcing safe behaviour whenever technology is used on site.
- creating a safe environment where pupils feel comfortable to say what they feel, without fear of getting into trouble and/or be judged for talking about something which happened to them online. • involving the Designated Safeguarding Lead (DSL) (Jennifer Cunningham) or a deputy (Victoria Pamuk/Debbie Withey/ Joanna Duckworth/Chantelle McCormack/Leanne Bolton) as part of planning

online safety lessons or activities to ensure support is in place for any pupils who may be impacted by the content.
- make informed decisions to ensure any online safety resources used with pupils is appropriate.

24. I will report any filtering breaches (such as access to illegal, inappropriate or harmful material) to the DSL in line with the school child protection policy.

25. I will respect copyright and intellectual property rights; I will obtain appropriate permission to use content, and if videos, images, text or music are protected, I will not copy, share or distribute or use them.

Use of Social Media and Mobile Technology

26. I have read and understood the school online safety policy which covers expectations regarding staff use of mobile technology and social media.

27. I will ensure that my online reputation and use of IT and information systems are compatible with my professional role and in line with the staff code of conduct, when using school and personal systems. This includes my use of email, text, social media and any other personal devices or mobile technology.

- I will take appropriate steps to protect myself online when using social media as outlined in the online safety policy.
- I am aware of the school expectations with regards to use of personal devices and mobile technology, including mobile phones as outlined in the online safety policy.
- I will not discuss or share data or information relating to pupils, staff, school business or parents/carers on social media.
- I will ensure that my use of technology and the internet does not undermine my professional role or interfere with my work duties and is in accordance with the school code of conduct and the law.

28. My electronic communications with current and past pupils and parents/carers will be transparent and open to scrutiny and will only take place within clear and explicit professional boundaries.

- I will ensure that all electronic communications take place in a professional manner via school approved and/or provided communication channels, such as a school email address or telephone number.
- I will not share any personal contact information or details with pupils, such as my personal email address or phone number.
- I will not add or accept friend requests or communications on personal social media with current or past pupils and/or parents/carers.
- If I am approached online by a pupil or parents/carer, I will not respond and will report the communication to my line manager and Designated Safeguarding Lead (DSL).
- Any pre-existing relationships or situations that compromise my ability to comply with the AUP will be discussed with the Head teacher.

29. If I have any queries or questions regarding safe and professional practice online either in school or off site, I will raise them with the DSL and/or the Head teacher.

30. I will not upload, download or access any materials which are illegal, such as child sexual abuse images, criminally racist material, adult pornography covered by the Obscene Publications Act.

31. I will not attempt to access, create, transmit, display, publish or forward any material or content online that is inappropriate or likely to harass, cause offence, inconvenience or needless anxiety to any other person.

32. I will not engage in any online activities or behaviour that could compromise my professional responsibilities or bring the reputation of the school into disrepute.

Policy Compliance

33. I understand that the school may exercise its right to monitor the use of information systems, including internet access and the interception of emails, to monitor policy compliance and to ensure the safety of pupils and staff. This monitoring will be proportionate and will take place in accordance with data protection, privacy and human rights legislation.

Policy Breaches or Concerns

34. I will report and record concerns about the welfare, safety or behaviour of pupils or parents/carers to the DSL in line with the school child protection policy (Via CPOMs).

35. I will report concerns about the welfare, safety or behaviour of staff to the Head teacher, in line with the whistleblowing policy.

36. I understand that if the school believe that unauthorised and/or inappropriate use of school systems or devices is taking place, the school may invoke its disciplinary procedures as outlined in the code of conduct.

37. I understand that if the school believe that unprofessional or inappropriate online activity, including behaviour which could bring the school into disrepute, is taking place online, the school may invoke its disciplinary procedures as outlined in the code of conduct.

38. I understand that if the school suspects criminal offences have occurred, the police will be informed.

I have read, understood and will abide by with the school's ICT Security & Acceptable Use Policy and this User Agreement.

Signed: …… Print Name: …… Date: ……..

Appendix 3 – Online Safety Activity Guidance for Staff

St Barnabas and St Paul's C of E Primary School

Online Safety Activity Issues

- Teachers need to ensure that all pupils have returned and signed the consent forms and Online Safety Rules.
- Always refer to online safety issues throughout your teaching. Do not teach once and then never refer back to the key messages.

Age groups likely to be involved in activities.	Activities using ICT.	Issues that may arise from this activity.	What do we need to tell the children – information/ expectations /rules /sanctions
Reception to KS2	Recording the spoken word	Children recording inappropriate images/ sounds/ video.	Ensure children understand the need to show consideration for others. In reception this could simply be asking each other before taking recording sound, images or video. For older children you will need to discuss the inappropriate use of images etc. including bullying.
	Recording video	Children record others who do not wish to be recorded.	Permission is sought from parents within the Online Safety Agreements. Make sure that children in your class have permission before publishing images and video of children on the school website.
	Taking photographs	Images should only be stored where they are not accessible to the public.	Teachers will need to monitor work and ensure that the children are aware of sanctions where images, sound or video are intentionally misused. Intentional misuse is a behaviour issue and should be dealt with as such.
		Publishing images/video of children.	Teachers need to check if consent has been provided.

	Using teacher directed web activities.	Clicking on other things after losing the site.	Ensure children know what to do if they lose the activity they are on. Children must be taught to minimise and tell and adult.

		Accidental access of unsuitable sites.	Children are taught what to do if they accidentally access unsuitable sites – as above.
KS1 to KS2	Navigating teacher selected websites.	Accidental or intentional access of unsuitable sites or information. ***A slight misspelling may result in children accessing content you do not want them to.***	Talk to the children about what to do if they accidentally access something that makes them feel uncomfortable – minimise & tell. Ensure that children understand that the internet has information on it that is not intended for children. Discourage from typing in URLs from the address bar, as incorrect spelling can take them to inappropriate sites. Intentional access of inappropriate content must be reported to the Online Safety Coordinator (I Rawat).
	Saving work on the school network. Accessing work from the network.	The computer is logged on as a teacher and gives the children access to materials that are not intended for them e.g. reports, plans etc. A computer is logged on as another child and they accidentally or intentionally save over another's work.	Network set up so children use pupil log-ins, or are aware of file saving protocol. Spend time explaining the need for user names and passwords. Intentionally accessing, saving over or deleting other children's files must be reported to the Online Safety Coordinator (I Rawat). Teachers must log out. There is data protection issue if pupils can access information the teacher has saved in their area.

KS1 to KS2	Using a children's search engine with guidance.	Accidental or intentional access of unsuitable sites.	Provide children with access to appropriate children's search engines. Children need to be taught to read the information under the links that the search engine has found. They should also take care to spell the search word correctly. If in doubt they should minimise their screen and inform a member of staff. Intentional access must be reported to the Online Safety Coordinator (I Rawat). ***Children should not use an adult search engine. Where an adult is using an adult search engine, they should check the results before using it in front of the children or save the required URL into a***

			document or as a favourite.
	Using email, messaging, forums restricted to the school's network or monitored by the teacher.	Children use technology to bully. Children communicate in an inappropriate manner. A child uses another child's logon.	Discuss keeping passwords safe and discuss what is appropriate to say in messages – remind of our school values and consider how they would expect to be treated and treat others accordingly. Online bullying will be addressed during the school's annual Safety Week and should also be discussed in PSHE where appropriate. Reinforce the Online Safety Rules regarding communication Intentional inappropriate use of electronic communication must be reported to the Online Safety Coordinator. ***Staff are aware that it is socially acceptable for children to use an informal/familiar manner when talking to friends using technology. In order to protect staff, a professional approach must be used in all electronic communications.***

	Using monitored discussion forums and social networking.	Children can accidentally get out of safe sites or activity.	Discuss with the children which sites to use and why. Staff should always check sites before they are used by children. Ensure that there are clear sanctions for inappropriate use as this is a behaviour issue.
KS2	Typing teacher specified URLs into the address bar.	Addresses spelt wrongly can lead to dubious sites	Teach children to take care with typing and check entries before submitting. To prevent this from happening, you can use a Word document to copy and paste URLs from list. Intentional access of inappropriate sites must be reported to the Online Safety Coordinator (I Rawat).
	Searching for images.	Images are not easy to filter and it is impossible to be 100% sure that a search will only reveal appropriate images.	Use child-friendly search engines and ideally check key words before asking the children to search. Ensure that children are aware of ambiguous terms and words as appropriate to their age and ability. Always preview accessible images for suitability. Children to minimise and tell, or click Hector if they are unsure. Images are often subject to copyright and it is important that children are taught to respect this law. Intentional access of inappropriate content must be reported to the Online Safety Coordinator (I Rawat). ***Be aware that no filtering system is entirely safe especially where images are concerned. There are many other ways of providing children with appropriate images. Teachers must take steps to ensure methods of accessing images are as safe as possible.***

Use of technology that is not recommended for primary aged children.	Independently accessing websites of the child's own choice without asking the teacher.	Intentional and unintentional access of unsuitable sites. Use of social networking sites that are not appropriate for use in primary schools. Children giving personal details to others on unmonitored sites.	Make sure children know teachers can (and will) check the history of websites. Intentional access must be reported to the Online Safety Coordinator (I Rawat). ***While it is important to develop a sense of responsibility in our children, an adult should always be present in the room when children are using the internet and be aware of what the children are accessing.***
	Independently using an adult search engine.	Accidental or intentional access of unsuitable sites	Make sure children know teachers can (and will) check the history of websites. Intentional access must be reported to the Online Safety Coordinator (I Rawat).
	Sending messages with mobile phones	Bullying using technology.	Ensure the children are aware that bullying, including using mobile phones is unacceptable and that whether in school or out of school inappropriate use may be reported to the police.
	for social purposes.	Intentionally or accidentally revealing mobile phone numbers.	Ensure that children are aware of the consequences of passing on their phone number or that of another child. This must be reported to the Online Safety Coordinator (I Rawat).

	Using unmonitored email or chat.	Children do not know who they are talking to. Intentionally or accidentally revealing information about themselves or others.	Whilst children should not use these facilities in school, it is important that they understand the risks and how to minimise them e.g. never agree to meet anyone without an adult present. These issues should be addressed using the Think You Know / other resources, and must be reported to the Online Safety Coordinator (I Rawat).

Reviewed and updated: September 2021 (J Cunningham/I Rawat)

Appendix 4 – Online Safety Audit

Has the school an Online Safety Policy that complies with current guidance?	
Date of latest update:	
The Policy was agreed by governors on:	
The Policy is available for staff at: teacher shared – policies / website / staff training sessions / safeguarding display	
And for parents at: On the school's website	
The Designated Lead Person for Safeguarding and Child Protection is: Jennifer Cunningham	
The Online Safety Coordinator is: Ismail Rawat	
Has Online Safety training been provided for both pupils & staff?	
Do all staff sign an ICT Code of Conduct on appointment?	

Do parents sign and return an agreement that their child will comply with the School Online Safety Rules?	

As part of the annual review, this quick self-audit will help the senior leadership team (SLT) assess whether the internet safety basics are in place to support a range of activities that might include those detailed within Appendix 3.

Have school Online Safety Rules been set for students?	
Are these Rules displayed in all rooms with computers?	
Internet access is provided by an approved educational internet service provider and complies with DfE requirements for safe & secure access?	
Has an ICT security audit been initiated by SLT, possibly using external expertise?	
Is personal data collected, stored and used according to the principles of the Data Protection Act?	

Completed by: **Date:**