*”Love one another as Jesus loved us” (John 13 v 34-35*)

**LANCASHIRE COUNTY COUNCIL**

Diocese of Blackburn

St. John's C.E. (V.A) School, Clayton

‘Learn, Pray, Care & Play’

Our church school through its Christian values and caring community seeks to inspire each individual to achieve and grow.

## Online Safety Policy

St John’s C.E. Primary understands that using online services is an important aspect of raising educational standards, promoting pupil achievement and enhancing teaching and learning. Our online safety policy highlights the need to educate children and young people about the benefits and risks of using technology. It provides safeguards and awareness that enable them to control their experiences. Our policy will operate in conjunction with other policies including those for Pupil Behaviour, Curriculum and data Protection.

The use of online services is embedded throughout the school; therefore, there are a number of controls in place to ensure the safety of pupils and staff.
The breadth of issues classified within online safety is considerable, but they can be categorised into three areas of risk:

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

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

The school’s online safety coordinator is Mrs Healey supported by the Online Safety Governor and the Computing Subject Leader.

*”Love one another as Jesus loved us” (John 13 v 34-35*)

Our school online safety policy has been written by the school, building on guidance from Lancashire Authority and agreed by governors.

## 1. Legal Framework

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

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

1.2. This policy operates in conjunction with the following school policies:

- *Social Networking Sites and Social Media Policy*
- *Acceptable User Policy*
- *Safeguarding and Child Protection Policy*
- *Anti-Bullying Policy*
- *PSHE Policy*
- *Staff Code of Conduct*
- *Behaviour and Discipline Policy*
- *Disciplinary Policy and Procedures*
- *Data Protection Policy*
- *Health and Safety Policy*
- *Computing Policy*
- *Respect For All Policy*

## 2. Roles and Responsibilities

1.1. The **governing board** is responsible for:

- Ensuring that this policy is effective and complies with relevant laws and statutory guidance.
- Ensuring the DSL's remit covers online safety.
- Reviewing this policy on an annual basis.
- Ensuring their own knowledge of online safety issues is up-to-date.
- Ensuring all staff undergo safeguarding and child protection training (including online safety) at induction.
- Ensuring that there are appropriate filtering and monitoring systems in place.

1.2. The **headteacher** is responsible for:

- Supporting the DSL and any deputies by ensuring they have enough time and resources to carry out their responsibilities in relation to online safety.

- Ensuring staff receive regular, up-to-date and appropriate online safety training and information as part of their induction and safeguarding training.
- Ensuring online safety practices are audited and evaluated.
- Supporting staff to ensure that online safety is embedded throughout the curriculum so that all pupils can develop an appropriate understanding of online safety.
- Organising engagement with parents to keep them up-to-date with current online safety issues and how the school is keeping pupils safe.
- Working with the DSL and governing board to update this policy on an annual basis.

1.3. The **DSL** is responsible for:

- Taking the lead responsibility for online safety in the school supported by the Online Safety Governor and the Computing Subject Leader.
  - Acting as the named point of contact within the school on all online safeguarding issues.
  - Undertaking training so they understand the risks associated with online safety and can recognise additional risks that pupils with SEND face online.
  - Liaising with relevant members of staff on online safety matters, e.g. the SENCO, Computing Subject Leader and ICT technicians.
  - Ensuring online safety is recognised as part of the school's safeguarding responsibilities and that a coordinated approach is implemented.
  - Ensuring appropriate referrals are made to external agencies, as required.
  - Staying up-to-date with current research, legislation and online trends.
  - Coordinating the school's participation in local and national online safety events, e.g. Safer Internet Day. National Online Safety.
  - Establishing a procedure for reporting online safety incidents and inappropriate internet use, both by pupils and staff.
  - Ensuring all members of the school community understand the reporting procedure.
  - Maintaining records of reported online safety concerns as well as the actions taken in response to concerns.
  - Monitoring online safety incidents to identify trends and any gaps in the school's provision and using this data to update the school's procedures.
  - Reporting to the governing board about online safety on a termly basis.
  - Working with the headteacher and governing board to update this policy on an annual basis.

1.4. **ICT technicians** are responsible for:

- Providing technical support in the development and implementation of the school's online safety policies and procedures.
- Implementing appropriate security measures as directed by the headteacher.
- Ensuring that the school's filtering and monitoring systems are updated as appropriate.

1.5. **All staff members** are responsible for:

- Taking responsibility for the security of ICT systems and electronic data they use or have access to.
- Modelling good online behaviours.
- Maintaining a professional level of conduct in their personal use of technology.
- Having an awareness of online safety issues.
- Reporting concerns in line with the school's reporting procedure.
- Where relevant to their role, ensuring online safety is embedded in their teaching of the curriculum.

1.6. **Pupils** are responsible for:

- Adhering to this policy and other relevant policies.
- Seeking help from school staff if they are concerned about something they or a peer has experienced online.
- Reporting online safety incidents and concerns in line with the procedures within this policy.

## 3. The Curriculum

3.1. Online safety is embedded throughout the curriculum; however, it is particularly addressed in the following subjects:

- PSHE and RSE
- Computing

3.2. Pupils are taught the underpinning knowledge and behaviours that can help them to navigate the online world safely and confidently regardless of the device, platform or app they are using.

3.3. Online safety teaching is always appropriate to pupils' ages and developmental stages.

3.4. The underpinning knowledge and behaviours pupils learn through the curriculum include the following:

- How to evaluate what they see online
- How to recognise techniques used for persuasion
- Acceptable and unacceptable online behaviour
- How to identify online risks
- How and when to seek support

These are taught through the Purple Mash curriculum and the "S.M.A.R.T. rules".

3.5. The online risks pupils may face online are always considered when developing the curriculum. The risks that are considered and how they are covered in the curriculum can be found in Appendix 1 of this policy.

3.6. The DSL is involved with the development of the school's online safety curriculum supported by the Online Safety Governor and the Computing Subject Leader.

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

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

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

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

3.10. Before conducting a lesson or activity on online safety, the class teacher and DSL consider the topic that is being covered and the potential that pupils in the class have suffered or may be suffering from online abuse or harm in this way. The DSL advises the staff member on how to best support any pupil who may be especially impacted by a lesson or activity.

3.11. Lessons and activities are planned carefully so they do not draw attention to a pupil who is being or has been abused or harmed online, to avoid publicising the abuse.

3.12. During an online safety lesson or activity, the class teacher ensures a safe environment is maintained in which pupils feel comfortable to say what they feel and are not worried about getting into trouble or being judged.

3.13. If a staff member is concerned about anything pupils raise during online safety lessons and activities, they will make a report in line with sections 15 and 16 of this policy.

3.14. If a pupil makes a disclosure to a member of staff regarding online abuse following a lesson or activity, the staff member will follow the reporting procedure outlined in sections 15 and 16 of this policy.

## 4. Staff Training

4.1. All staff receive safeguarding and child protection training, which includes online safety training, during their induction.

4.2. Online safety training for staff is updated annually.

4.3. In addition to this training, staff also receive regular online safety updates as required and at least annually.

4.4. The DSL and any deputies undergo training to provide them with the knowledge and skills they need to carry out their role, this includes online safety training. This training is updated at least every two years.

4.5. In addition to this formal training, the DSL and any deputies receive regular online safety updates to allow them to keep up with any developments relevant to their role. In relation to online safety, these updates allow the DSL and their deputies to:

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

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

4.7. Staff are required to adhere to the Staff Code of Conduct at all times, which includes provisions for the acceptable use of technologies and the use of social media.

4.8. All staff are informed about how to report online safety concerns, in line with sections 15 and 16 of this policy.

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

## 5. Educating Parents

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

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

- Parents' evenings
- Safer Internet Day videos shared on the class pages of the school website
- Newsletters
- Links to online safety on school website
- National Online Safety advice on the school website (links on newsletters)

5.3. Parents are sent a copy of the Acceptable Use Agreement at the beginning of each academic year and are encouraged to go through this with their child to ensure their child understands the document and the implications of not following it. They are also required to sign the 'Home/School agreement' which refers to online safety.

## 6. Classroom Use

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

- Computers
- iPads
- Internet
- Email

6.2. Prior to using any websites, tools, apps or other online platforms in the classroom, or recommending that pupils use these platforms at home, the class teacher always reviews and evaluates the resource.

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

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

## 7. Internet Access

7.1. Pupils, staff and other members of the school community are only granted access to the school's internet network once they have read and signed the Acceptable Use Agreement. They must also read the Social Media Policy and act accordingly.

7.2. A record is kept of users who have been granted internet access in the school office.

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

## 8. Filtering and Monitoring Online Activity

8.1. The governing board ensures the school's ICT network has appropriate filters and monitoring systems in place.

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

8.3. The governing board ensures 'over blocking' does not lead to unreasonable restrictions as to what pupils can be taught with regards to online teaching and safeguarding.

8.4. P3, as part of their IT contract with the school, undertakes monthly checks on the filtering and monitoring systems to ensure they are effective and appropriate.

8.5. Requests regarding making changes to the filtering system are directed to the headteacher.

8.6. Prior to making any changes to the filtering system, ICT technicians and the DSL conduct a risk assessment.

8.7. Any changes made to the system are recorded by ICT technicians.

8.8. Reports of inappropriate websites or materials are recorded in the office and then reported to an ICT technician immediately, who investigates the matter and makes any necessary changes.

8.9. Deliberate breaches of the filtering system are reported to the DSL and ICT technicians, who will escalate the matter appropriately. There is a book to record any incidences in the school office and this will be reported to the governing body each term.

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

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

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

8.13. The school's network and school-owned devices are appropriately monitored.

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

8.15. Concerns identified through monitoring are reported to the DSL who manages the situation in line with sections 15 and 16 of this policy.

## 9. Network Security

9.1. Technical security features, such as anti-virus software, are kept up-to-date and managed by ICT technicians.

9.2. Firewalls are switched on at all times.

9.3. ICT technicians review the firewalls on a fortnightly basis to ensure they are running correctly, and to carry out any required updates.

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

9.5. Staff members and pupils report all malware and virus attacks to ICT technicians.

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

9.7. Pupils in KS2 and above are provided with their own unique username and private passwords.

9.8. Staff members and pupils are responsible for keeping their passwords private.

9.9. Passwords have a minimum and maximum length and require a mixture of letters, numbers and symbols to ensure they are as secure as possible.

9.10. Users are not permitted to share their login details with others and are not allowed to log in as another user at any time.

9.11. Users are required to lock access to devices and systems when they are not in use.

9.12. Users inform ICT technicians if they forget their login details, who will arrange for the user to access the systems under different login details.

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

## 10. Emails

10.1. Staff are given approved school email accounts and are only able to use these accounts at school and when doing school-related work outside of school hours.

10.2. Prior to being authorised to use the email system, staff must agree to and sign the relevant acceptable use agreement.

10.3. Any email that contains sensitive or personal information is only sent using secure and encrypted email. Staff members and pupils are required to block spam and junk mail and report the matter to ICT technicians.

## 11. Social Networking (Please also refer to the Social media Policy)

11.1. Access to social networking sites is filtered as appropriate.

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

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

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

11.5. Staff receive annual training on how to use social media safely and responsibly.

11.6. Staff are not permitted to communicate with pupils or parents over social networking sites and are reminded to alter their privacy settings to ensure pupils and parents are not able to contact them on social media.

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

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

## 12. The School Website

12.1. The headteacher is responsible for the overall content of the school website – they will ensure the content is appropriate, accurate, up-to-date and meets government requirements.

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

12.3. Personal information relating to staff and pupils is not published on the website.

## 13. Use of school-owned devices

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

- Laptop
- iPad

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

13.3. School-owned devices are used in accordance with the Device User Agreement.

13.4. Staff and pupils are not permitted to connect school-owned devices to public Wi-Fi networks.

13.5. All school-owned devices are password protected.

13.6. All school-owned devices are fitted with software to ensure they can be remotely accessed, in case data on the device needs to be protected, retrieved or erased.

13.7. ICT technicians review all school-owned devices on a monthly basis to carry out software updates and ensure there is no inappropriate material on the devices.

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

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

## 14. Use of personal devices

14.1. Any personal electronic device that is brought into school is the responsibility of the user. Staff members are not permitted to use their personal devices during lesson time, other than in an emergency.

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

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

14.4. If a member of staff is thought to have illegal content saved or stored on a personal device, or to have committed an offence using a personal device, the headteacher will inform the police and action will be taken in line with the Allegations of Abuse Against Staff Policy.

14.5. Pupils are not permitted to bring mobile devices into school.

14.6. The headteacher may authorise the bringing in and/or use of mobile devices by a pupil for safety or precautionary use.

14.7. Pupils' devices can be searched, screened and confiscated in accordance with the *Policy for*

*Electronic Devices - Searching & Deletion*

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

14.9. Appropriate signage is displayed to inform visitors to the school of the expected use of personal devices.

14.10. Any concerns about visitors' use of personal devices on the school premises are reported to the DSL.

## 15. Managing Reports of Online Safety Incidents

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

- Staff training
- The online safety curriculum
- Assemblies

15.2. Concerns regarding a staff member's online behaviour are reported to the headteacher who decides on the best course of action in line with the relevant policies, e.g. Staff Code of Conduct, Allegations of Abuse Against Staff Policy and Disciplinary Policy and Procedures.

15.3. Concerns regarding a pupil's online behaviour are reported to the DSL who investigates concerns with relevant staff members, e.g. the headteacher and ICT technicians.

15.4. Concerns regarding a pupil's online behaviour are dealt with in accordance with relevant policies depending on their nature, e.g. Behavioural Policy and Child Protection and Safeguarding Policy.

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

15.6. All online safety incidents and the school's response are recorded by the DSL.

15.7. Section 16 of this policy outlines how the school responds to specific online safety concerns, such as cyberbullying and peer-on-peer abuse.

## 16. Responding to Specific Online Safety Concerns

Cyberbullying

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

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

16.3. Information about the school's full response to incidents of cyberbullying can be found in the Cyberbullying Policy.

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

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

- Non-consensual sharing of sexual images and videos

- Sexualised cyberbullying
- Online coercion and threats
- Unwanted sexual comments and messages on social media
- Online sexual exploitation

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

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

16.7. Information about the school's full response to incidents of online peer-on-peer abuse can be found in the Child Protection and Safeguarding Policy.

Upskirting

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

16.9. A "specified purpose" is namely:

- Obtaining sexual gratification (either for themselves or for the person they are enabling to view the victim's genitals, buttocks or underwear).
- To humiliate, distress or alarm the victim.

16.10. "Operating equipment" includes enabling, or securing, activation by another person without that person's knowledge, e.g. a motion activated camera.

16.11. Upskirting is not tolerated by the school.

16.12. Incidents of upskirting are reported to the DSL who will then decide on the next steps to take, which may include police involvement, in line with the Child Protection and Safeguarding Policy.

Youth produced sexual imagery (sexting)

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

16.14. All concerns regarding sexting are reported to the DSL.

16.15. Following a report of sexting, the following process is followed:

The process below is recommended in the UK Council for Child Internet Safety's (UKCCIS) 'Sexting in schools and colleges: Responding to incidents and safeguarding young people' guidance.

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

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

16.17. If a staff member believes there is a good reason to view youth produced sexual imagery as part of an investigation, they discuss this with the headteacher first.
16.18. The decision to view imagery is based on the professional judgement of the DSL and always complies with the Child Protection and Safeguarding Policy.

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

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

16.21. Viewing and deleting imagery is carried out in line with the *Policy for Electronic Devices - Searching & Deletion*

<u>Online abuse and exploitation</u>
16.22. Through the online safety curriculum, pupils are taught about how to recognise online abuse and where they can go for support if they experience it.

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

16.24. All concerns relating to online abuse and exploitation, including child sexual abuse and exploitation and criminal exploitation, are reported to the DSL and dealt with in line with the Child Protection and Safeguarding Policy.

Online hate

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

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

Online radicalisation and extremism

16.27. The school's filtering system protects pupils and staff from viewing extremist content.

16.28. Concerns regarding a staff member or pupil being radicalised online are dealt with in line with the Child Protection and Safeguarding Policy and Prevent Duty.

## 17. Monitoring and Review

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

17.2. The governing board, headteacher and DSL review this policy in full on an annual basis and following any online safety incidents.

17.3. The next scheduled review date for this policy is September 2026.

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