Sacred Heart Primary Catholic School

Online Safety

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 (2024) 'Keeping children safe in education'
- DfE (2023) 'Teaching online safety in school'
- DfE (2023) 'Searching, screening and confiscation'
- National Cyber Security Centre (2020 reviewed) 'Cyber Security: Small Business Guide'
- UK Council for Internet Safety (2020) 'Education for a Connected World'
- UK Council for Internet Safety (March 2023) 'Sharing nudes and Semi-nudes and how to respond'

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

- Acceptable Use Agreement
- Child Protection and Safeguarding Policy
- Staff Code of Conduct
- Behaviour Policy including anti bullying
- Disciplinary Policy and Procedures
- Data Protection Policy

2. Roles and responsibilities

2.1. 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.

2.2. The Principal 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 students 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 students safe.
- Working with the DSL and governing board to update this policy on an annual basis.

2.3. The DSL is responsible for:

- Taking the lead responsibility for online safety in the school.
- 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 students with SEND and vulnerable pupils face online.
- Liaising with relevant members of staff on online safety matters, e.g. the SENDCO 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.

- Establishing a procedure for reporting online safety incidents and inappropriate internet use, both by students 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 Principal and governing board to update this policy on an annual basis.
- Highlighting training and tips to staff and parents, communicated via Mental Health and Safeguarding Newsletters

2.4. ICT technicians:

- 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 Principal.
- Ensuring that the school's filtering and monitoring systems are updated as appropriate.

2.5. 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.

2.6. Students are responsible for:

- Adhering to this policy, the Acceptable Use Agreement 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:

- RSHE (via the Teacher/Tutor Time)
- Form time SMSVC
- Computing lessons

The underpinning knowledge and behaviours students 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

3.2 The online risks students 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.

3.3 The DSL is involved with the development of the school's online safety curriculum.

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

3.5 Class teachers review external resources prior to using them for the online safety curriculum, to ensure they are appropriate for the cohort of students. 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 students?

Are they appropriate for students' developmental stage?

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

3.7 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 students 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 student who may be especially impacted by a lesson or activity.

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

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

3.14. If a staff member is concerned about anything students raise during online safety lessons and activities, they will make a report directly to a school DSL.

3.15. If a student 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 the school safeguarding 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 and is delivered in line with advice from local safeguarding partners and National Online Safety.

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 through National Online Safety. 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 students safe while they are online at school.
- Recognise the additional risks that students 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 students 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:

- School website
- Social media posts
- Mental Health and Safeguarding Newsletters
- Links sent via email and other forms of communication.

A copy of the acceptable use agreement is provided via the school website.

6. Classroom use

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

- Computers
- Laptops
- Tablets
- Internet
- Email
- Cameras
- Visualisers

6.2. Prior to using any websites, tools, apps or other online platforms in the classroom, or recommending that students 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. Students are supervised when using online materials during lesson time – this supervision is suitable to their age and ability.

7. Internet access

7.1. Students, 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.

7.2. A record is kept of users who have been granted internet access on the shared drive on the school's ICT network.

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 students' ages, the number of students using the network, how often students 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 students can be taught with regards to online teaching and safeguarding.

8.4 ICT technicians undertake 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 Principal.

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

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

8.9. Reports of inappropriate websites or materials are made to an ICT technician immediately, who investigates the matter and makes any necessary changes.

8.10. Deliberate breaches of the filtering system are reported to the DSL and ICT technicians who will escalate the matter appropriately.

8.11. If a student has deliberately breached the filtering system, they will be disciplined in line with the Behaviour Policy.

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

8.13. 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.

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

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

8.16. 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 engineers.

9.2. Firewalls are switched on at all times.

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

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

9.5. Staff members and students report all malware and virus attacks to ICT engineers.

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

9.7. Students in class year or key stage and above are provided with their own unique username and private passwords.

9.8. Staff members and students 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.

10. Passwords expire after 90 days, after which users are required to change them.

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

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

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

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

9.15. Full details of the school's network security measures can be found in the Data and E-Security Breach Prevention and Management Plan.

10. Emails

10.1. Access to and the use of emails is managed in line with the Data Protection Policy, Acceptable Use Agreement and Confidentiality Policy.

10.2. Staff and students 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.

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

10.4. Personal email accounts are not permitted to be used on the school site for the purposes of sending school emails to personal addresses.

10.5. Any email that contains sensitive or personal information is only sent using secure and encrypted email.

10.6. Staff members and students are required to block spam and junk mail, and report the matter to ICT engineers.

10.7. The school's monitoring system can detect inappropriate links, malware and profanity within emails – staff and students are made aware of this.

10.8. Chain letters, spam and all other emails from unknown sources are deleted without being opened.

10.9. Any cyberattacks initiated through emails are managed in line with the Data and E-Security Breach Prevention and Management Plan.

11. Social networking

Personal use:

11.1. Access to social networking sites via the school's WiFi is filtered as appropriate for both staff and students.

11.2. Staff and students 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 students or parents over social networking sites and are reminded to alter their privacy settings to ensure students and parents are not able to contact them on social media.

11.7. Students 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. Behaviour with Anti Bullying Policy, Staff Code of Conduct.

Use on behalf of the school:

11.9. The use of social media on behalf of the school is conducted in line with the Social Media Policy.

11.10. The school's official social media channels are only used for official educational or engagement purposes.

11.11. Staff members must be authorised by the Principal to access to the school's social media accounts.

11.12. All communication on official social media channels by staff on behalf of the school is clear, transparent and open to scrutiny.

11.13. The Staff Code of Conduct contains information on the acceptable use of social media – staff members are required to follow these expectations at all times.

12. The school website

12.1. The Principal 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 students is not published on the website.

12.4. Images and videos are only posted on the website if the provisions in the Photography Policy are met.

13. Use of school-owned devices

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

- Laptop

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

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

13.4. Staff and students 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 mobile school-owned devices are fitted with tracking software to ensure they can be retrieved if lost or stolen.

13.7. 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.

13.8. ICT engineers review all school-owned devices and have the right to review devices on an adhoc basis.

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

13.10. Staff members or students found to be misusing school-owned devices are disciplined in line with the Disciplinary Policy and Procedure and Behaviour Policy.

14. Use of personal devices

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.

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

14.1 Staff members report concerns about their colleagues' use of personal devices on the school premises to the Principal.

14.2 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.

14.7. Students are not permitted to use their personal devices during lesson time (unless permission is expressly given by the class teacher) or when moving between lessons.

14.8. If a student needs to contact their parents during the school day, they are allowed to use the phone in the school office.

14.9. The headteacher may authorise the use of mobile devices by a student for safety or precautionary use.

14.10. Students' devices can be searched, screened and confiscated in accordance with the Searching, Screening and Confiscation Policy.

14.11. If a staff member reasonably believes a student'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.

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

14.13. 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 students 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 student's online behaviour are reported to the DSL who investigates concerns with relevant staff members, e.g. the headteacher and ICT engineers.

15.4. Concerns regarding a student's online behaviour are dealt with in accordance with relevant policies depending on their nature, e.g. Behaviour 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

16 Cyberbullying

16.1. Cyberbullying, against both students 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 child on child 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 child – on - child 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 child – on - child 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 DSL holds an initial review meeting with appropriate school staff
- Subsequent interviews are held with the students 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 student at risk of harm
- At any point in the process if there is a concern a student 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, students 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 Searching, Screening and Confiscation Policy.

Online abuse and exploitation

16.22. Through the online safety curriculum, students 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 and Adult Code of Conduct.

Online radicalisation and extremism

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

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

17. Monitoring and review

17.1. The school recognises that the online world is constantly changing; therefore, the DSL, ICT engineers 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 2025.**

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

18. Artificial Intelligence

Generative artificial intelligence (AI) tools are now widespread and easy to access. Staff, pupils and parents/carers may be familiar with generative chatbots such as ChatGPT and Google Bard.

We recognise that AI has many uses to help pupils learn, but may also have the potential to be used to bully others. For example, in the form of 'deepfakes', where AI is used to create images, audio or video hoaxes that look real. This includes deepfake pornography: pornographic content created using AI to include someone's likeness.

We will treat any use of AI to bully pupils in line with our behaviour policy.

Staff should be aware of the risks of using AI tools whilst they are still being developed and should carry out a risk assessment where new AI tools are being used by the school.

19. Pupil Responsibility

When I use the school's ICT systems (like computers or Ipads) and get onto the internet in school I will:

- Ask a teacher or adult if I can do so before using them
- Only use websites that a teacher or adult has told me or allowed me to use
- Tell my teacher immediately if:
    - I select a website by mistake
    - I receive messages from people I don't know
    - I find anything that may upset or harm me or my friends
- Use school computers for school work only
- Be kind to others and not upset or be rude to them
- Look after the school ICT equipment and tell a teacher straight away if something is broken or not working properly
- Only use the username and password I have been given
- Try my hardest to remember my username and password
- Never share my password with anyone, including my friends
- Never give my personal information (my name, address or telephone numbers) to anyone without the permission of my teacher or parent/carer
- Save my work on the school network
- Check with my teacher before I print anything
- Log off or shut down a computer when I have finished using it

I agree that the school will monitor the websites I visit and that there will be consequences if I don't follow the rules.

Appendix A

Academic Excellence,
Social Awareness,
Spiritual Development.

Bishop Walsh Catholic School
Wylde Green Road, Sutton Coldfield B76 1QT
E: enquiry@bishopwalsh.net
T: 0121 351 3215 | F: 0121 313 2142
W: www.bishopwalsh.net
Principal: Mrs N. Brodie
Acting Catholic Senior Executive Leader (CSEL): Mr M. Emery

Equipment Release Form

By signing below, I acknowledge that I have received the following equipment for work purposes. I will carry out due diligence and look after the equipment and data. I understand that I am not to upload personal pictures to the desktop and I will keep the laptop safe when off site in my home (not left in any vehicles). I agree to report any concerns or damages immediately to IT.

Description of Item	Serial Number

_____Date_____
Staff Signature

_____Date_____
IT Signature

Admin Use Only

Check Out Date_____

Date Returned_____

Appendix B St John Paul II Multi-Academy

Staff Rules for Responsible ICT Usage.

Staff Rules for Responsible ICT Usage

The ICT devices and systems within the St John Paul II Multi Academy are owned by the Academy. These Responsible ICT Usage Rules help to protect students, staff*, visitors* and the Academy by clearly stating what use of the devices and systems resources is acceptable and what is not.

Access/Use

1. All users are advised to familiarise themselves with the Academy "ICT and Internet Safety Policy (change to e-safety), Data Protection Policy, GDPR Policy, BYOD Policy, available on the Academy website http://johnpaulii.co.uk
2. These rules apply to Academy owned devices and personal owned ICT equipment that you use to access Academy systems and any equipment used in conjunction with the devices and systems
3. Irresponsible use may result in the loss of access to these Devices and systems.
4. The use of these Devices and systems must be appropriate to the student's education or to staff/visitor professional activity.
5. The use of the Internet must be appropriate to the student's education or to staff/visitor professional activity.
6. Network access must be made via the user's authorised account and password, which must not be given to, or used by, any other person – except supervised in-class. The use of designated teacher/staff devices and systems is prohibited to students.
7. The Academy systems may not be used for private purposes, personal financial gain, gambling political purposes or commercial advertising.
8. Accidental access to inappropriate websites/material will not be penalised; however, users must report the circumstances of this occurring to the Principal of the School that has allocated the Academy device or access to their systems as soon as possible.

Communication

1. The Academy provided email system, must be used for all school related work and communication.
2. Email should be written carefully and politely, particularly as messages may be forwarded or printed and be seen by unexpected readers.
3. Users are responsible for email they send and for contacts made.
4. Anonymous messages and chain letters are not permitted.
5. The use of unmonitored chat rooms and social networking sites, to communicate with other school users, is not allowed.
6. Communication with other school users is ONLY permitted through monitored school sanctioned systems including School Email and Learning Platform.

Copyright/Personal Information

1. Copyright and intellectual property rights must be respected.
2. When working with digital images and video, school recording equipment must be used, rather than personal recording equipment.
3. Before any images of students/staff are displayed on websites or Academy agreed social networking sites and only if the user has been trained on the sites profile security setting, knows how to access the list of photo permission relevant to the Academy school/elements.
4. Given permission to do this by the Principal of the Academy school/elements.

Security

1. The Academy devices, system and Internet security must be respected; it is a criminal offence to use a device, system and/or internet not for the purpose it was issued for or access given for.
2. The Academy devices and system that are taken or accessed off site must when requested to be allowed to update, to ensure that security updates, anti-virus software, and monitoring software updates; are kept up-to-date *(if any issues arise during or after these update these must be reported to the Academy's School/elements IT support team)*

The Academy may exercise its right to monitor the use of the devices and systems, including access to websites, the interception of email and the deletion of inappropriate materials where it believes unauthorised use of the Academy devices system is or may be taking place, or the system is or may be being used for criminal purposes or for storing unauthorised or unlawful text, imagery or sound.

Staff Agreement

I have read and understand the "Staff Rules for Responsible ICT Usage. I will use devices, systems, internet and email in a responsible way and obey these rules at all times.

I acknowledge that I have been advised to familiarise myself with the Academy's Policy indicated in item (1) under **Access/Use**", available on the Academy website http://johnpaulii.co.uk.

I understand that the Academy will take all reasonable precautions to ensure pupils and staff/visitors cannot access inappropriate materials.

I understand that the Academy cannot be held responsible for the nature or content of materials accessed through the internet.

I agree that the Academy is not liable for any damages arising from use of the devices and systems allocated to the user.

Staff Signature:_____**Date:** _____

St John Paul II Multi Academy
Be not afraid

"Do not be afraid. Open wide the doors for Christ."

SACRED HEART
CATHOLIC PRIMARY SCHOOL