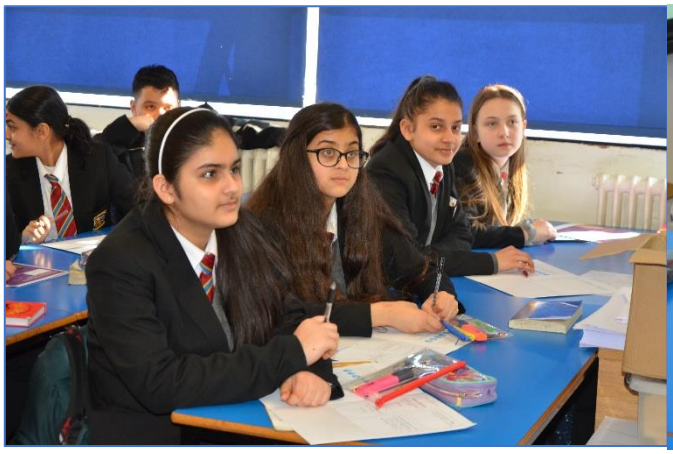
Saint John Wall Catholic School

A Catholic School For All

Mission Statement

'To educate each and every unique child in our care to hear and respond to what God calls them to be'



Internet and E-Technologies

Policy for Staff & Pupils

"God will equip you with everything good that you may do his will"

Hebrews 13:21

BIRMINGHAM CITY COUNCIL

APRIL Ofsted Good Provider 2017

November Section 48 Catholic Ethos Report 'Outstanding' 2017

MODEL E-SAFETY POLICY FOR SCHOOLS

*indicates points at which each school must insert the arrangements applicable in that school

1. Introduction

1.1 The governing body of Saint John Wall Catholic School has adopted this policy to help the school meet its responsibilities for safeguarding and educating children, for regulating the conduct of employees and for complying with legislation covering the use of information and communication technologies and digital and mobile devices.

1.2 This policy was adopted by the governing body on 7 July 2021 and will be reviewed annually in the light of guidance from the local authority or earlier if the local authority issues further guidance in the light of particular circumstances or developments in information and communication technology.

2. Basic principles

2.1 In adopting this policy the governing body has taken into account the expectation by Ofsted that rigorous e-safety policies and procedures are in place in the school, written in plain English, with contributions from the whole school, updated regularly and ratified by governors.

2.2 The policy applies to all members of the school community, including staff, pupils, volunteers, parents and carers, governors, visitors and community users who have access to, and are users of, the school's information and communication technology systems or who use their personal devices in relation to their work at the school.

2.3 The governing body expects the headteacher to ensure that this policy is implemented, that training in e-safety is given high priority across the school, that consultations on the details of the arrangements for e-safety continue with all employees on a regular basis, and that any necessary amendments to this policy are submitted to this governing body for approval.

2.4 The principal context for this policy is the need to safeguard children. It will be applied in conjunction with the procedure for safeguarding children approved by the Birmingham Safeguarding Children Board. It will also be applied in conjunction with the school's behaviour and anti-bullying policies for pupils and with the rules and procedures governing the conduct of employees.

2.5 The governing body expects the headteacher to arrange for this policy to be published to all employees and volunteers in the school and for necessary instructions and guidance, particularly on acceptable use, to be given to pupils in a manner suited to their ages and abilities.

3. Roles and responsibilities

Governing body

3.1 The governing body will consider and ratify this e-safety policy, and review it annually in the light of guidance from the local authority, or sooner if the local authority issues new guidance in the light of particular circumstances or developments in information and communication technology. Governors are expected to follow the policy in the same way as volunteers are expected to follow it, including participating in e-safety training if they use information and communication technology in their capacity as school governors.

3.2 Governors are responsible for ensuring that proper procurement procedures are used if they decide to purchase information technology services from an external contractor and that DfE or other reputable specialist advice is taken on the specification for those services to ensure proper security and safeguarding of children.

Headteacher

3.3 The headteacher is responsible for ensuring that

- the governing body is offered appropriate support to enable this policy and its application to be reviewed regularly, and to ensure that other school policies, including that on pupils' behaviour, take account of this e-safety policy;
- the governing body is given necessary advice on securing appropriate information and communication technology systems;
- the school obtains and follows DfE or other reputable guidance on information and communication technology to support this policy;
- the school has a designated senior person to co-ordinate e-safety and that this person has adequate support from, and provides support to, other employees, particularly the designated senior person for safeguarding;
- there is effective consultation with all employees, and other users of the school's information and communication technology systems, to take account of the particular features of those systems and educational, technical and administrative needs;
- the school provides all employees with training in e-safety relevant to their roles and responsibilities and that training is also provided to volunteers and school governors who use information and communication technology in their capacity as volunteers or governors, as the case may be;
- pupils are taught e-safety as an essential part of the curriculum;
- the senior leadership team is aware of the procedures to be followed in the event of a serious e-safety incident, including an allegation made against an employee, and that all employees know to whom they should report suspected misuse or a problem ;
- records are kept of all e-safety incidents and that these are reported to the senior leadership team;
- necessary steps have been taken to protect the technical infrastructure and meet technical requirements of the school's information and communication technology systems;
- there is appropriate supervision of, and support for, technical staff;
- any outside contractor which manages information technology for the school undertakes all the safety measures which would otherwise be the responsibility of the school to the standard required by the school and is fully aware of this policy and that any deficiencies are reported to the body which commissioned the contract.

Other employees

3.4 Other employees are responsible for

- undertaking such responsibilities as have been delegated by the headteacher commensurate with their salary grade and job descriptions;
- participating in training in e-safety provided by the school and in consultations about this policy and about its application, including e-safety within the curriculum;
- using information and communication technology in accordance with this policy and the training provided;
- reporting any suspected misuse or problem to the person designated by the school for this purpose.

Pupils

3.5 Pupils are expected to use information and communication technology systems and devices as they have been taught and in accordance with the school's behaviour policy and the instructions given to them by staff.

Other users

3.6 Volunteers, including governors, who help in the school and who use information and communication technology systems and devices in helping the school are expected to

- participate in training in e-safety provided by the school and in consultations about this policy and about its application, including e-safety within the curriculum;
- use information and communication technology in accordance with this policy and the training provided;
- report any suspected misuse or problem to the person designated by the school for this purpose.

Parents

3.7 Parents who help in the school as volunteers are covered by 3.6 above. Parents who are not voluntary helpers in the school are nonetheless subject to the law in the event of misuse of information and communication technology.

4. Acceptable use

4.1 The use of information and communication technology should follow the following general principles:

- This policy should apply whether systems are being used on or off the school premises.
- The school's information and communication technology systems are intended primarily for educational use and the management and administration of the school. During work breaks appropriate, reasonable personal use is permitted.
- GDPR legislation must be followed.
- Users must not try to use systems for any illegal purposes or materials.
- Users should communicate with others in a professional manner.
- Users must not disclose their password and they should not write it down or store it where it is possible that another person might steal it. Users must not attempt to use another person's user-name or password.
- Users must report as soon as possible any apparently illegal, inappropriate or harmful material or event to the person designated by the school.

4.2 Employees, volunteers and governors should:

- not open, copy, remove or alter any other user's files without that person's express permission;
- only take and/or publish images of other people with their permission, or, in the case of pupils, the permission of their parents or guardians;
- when recording or publishing such images for educational purposes should not attach to those images any names or other personal information enabling identification;
- as far as possible communicate with pupils and parents only through the school's official communication systems and not publish personal contact details through those systems;
- if they occupy a senior post in which they need to keep e-mail and other messages confidential, ask the school for a separate e-mail address for this purpose;

- if they use personal devices during their work (subject to the agreement of the school in the case of employees), ensure that the systems which they use are secure, protected with passwords and encrypted;
- not use personal social networking sites through the school's information and communication technology systems;
- not open any hyperlinks in, or attachments to, e-mails, unless the source is known and trusted;
- ensure that their data is backed-up regularly in accordance with the rules of the school's systems;
- only download or upload large quantities of information if they have permission to do so, in order to avoid overloading the school's systems
- not try to install any programmes or alter any computer settings unless this is allowed under the rules for the school's information and communication technology systems;
- not deliberately disable or damage any information and communication technology equipment;
- report any damage or faults to the appropriate member of staff.

4.3 Use of social media networks or sites, whether by pupils or employees, should be subject to the same standards as the school would expect for behaviour and conduct generally (as set out in the school's code of conduct for support staff and the Teachers' Standards for teachers). The school accepts the separation of private life and work and will not concern itself with people's private lives unless it appears that the law has been broken, or that an employee is in breach of contract, or that the school is, or will be, brought into disrepute.

5. Education and training

5.1 Education and training in e-safety will be given high priority across the school.

5.2 The education of pupils in e-safety is an essential part of the school's e-safety provision and will be included in all parts of the curriculum.

5.3 The school will offer education and information to parents, carers and community users of the school about e-safety.

5.4 Suitable training will be provided through the school for all employees, as part of induction and subsequently during their employment in the school. There will be a regular review of the training needs of all staff and the content of training should be kept up to date. The training will be linked to training about child protection and data protection. It will cover related matters such as the law on copyright of electronic materials.

5.5 Volunteers and governors who use information and communication technology during their work will be offered the same training as employees.

6. GDPR

6.1 The school will ensure that its information and communication technology systems are used in compliance with current GDPR legislation and that all users are made aware of the school's data protection policy, including the requirement for secure storage of information.

7. **Technical aspects of e-safety**

7.1 The school will seek to ensure that the information and communication technology systems which it uses are as safe and secure as is reasonably possible by taking reputable advice and guidance on the technical requirements for those systems.

7.2 The school will undertake regular reviews of the safety and security of its information and communication technology systems.

7.3 Particular attention will be paid to secure password protection and encryption for devices located in the school and mobile devices.

7.4 The school's systems will also provide for filtering internet access for all users (accessing internet from the premises), preventing access to illegal content, and with additional filtering for different groups of users for inappropriate content.

7.5 The school will ensure that its information and communication technology systems include standard, automated monitoring for illegal materials, profanity, and unsolicited materials (generally known as 'spam'). It should safeguard children and adults against inappropriate use. It should provide the headteacher and senior leadership team with regular reports to indicate whether or not there have been any incidents.

7.6 Additional monitoring may take place as part of an investigation following evidence of apparent misuse.

8. **Dealing with incidents**

8.1 Any suspicions of misuse or inappropriate activity related to child protection should be reported as prescribed in the Safeguarding Board's child protection procedures.

8.2 Any suspicions of other illegal activity should be reported to the headteacher, who should take advice from appropriate persons (according to the nature of the suspected activity and the individuals apparently involved) and, depending on the advice and the outcome of preliminary investigations, should report alleged criminal activity to the police and may also instigate disciplinary procedures.

8.3 Suspicions of inappropriate, as distinct from illegal, use of information and communication technology should be reported to the headteacher or other designated member of the senior leadership team for investigation and appropriate action. This may lead to informal management discussions, improved training or, depending on the nature of the alleged misuse, investigation under the disciplinary procedure for employees, or the school's behaviour policy for pupils.

Appendix 1

E-SAFETY POLICY FOR STAFF

The use of Internet, digital and information technologies are powerful tools, which open up new opportunities for everyone. However, 'e' technology can expose our pupils to danger.

This policy is written to ensure that our pupils are able to use the Internet and related communication technologies appropriately and safely.

This policy is linked with policies on Child Protection, Health & Safety, Bullying and Copyright.

It is a policy supported by Governors, teachers, parents and pupils to ensure that all are aware of the safety issues and adhere to its guidelines when using Internet, digital and information technologies, which we will refer to as 'E' technologies in the policy.

Risks involved with 'E' technologies are:

- Copyright infringement.
- Obsessive use of Internet and ICT.
- Exposure to inappropriate materials.
- Physical danger and sexual abuse.
- Online gambling.
- Identity theft.

Pupils must be able to critically think and judge inappropriate behaviours to ensure they are safe and legal when using the Internet and related technologies. Staff must also be aware of risks that they can be exposed to whilst using 'E' technologies.

To create a safe ICT learning environment the school will include:

- An infrastructure of whole school awareness, designated responsibilities, policies and procedures.
- An effective range of technological tools.
- A comprehensive Internet safety education programme for the whole school.

Responsibilities

1. The overall responsibility for the day to day administration is with the Headteacher, under the direction of the Governing Body.
2. Network managers have responsibilities to establish and maintain a safe ICT learning environment for the school by means of electronic security systems, supervision of pupils' work, appropriate processes for responding to illegal materials and reporting breaches
3. **Curriculum Coordinator of ICT**
   Should support other Curriculum Coordinators in ensuring a consistent approach to 'E' Safety in each curriculum area.
4. **All Curriculum Coordinators and Teachers** will ensure compliance of Internet safety policy embedding into the context of curriculum. All curriculum staff should ensure that safety measures are appropriate for the particular situation and subject, and should be evident in their own department policy.

5. **Pastoral Coordinators**
   All Pastoral Coordinators act as first point of contact regarding Internet safety and ensure any instances of ICT misuse, accidental or deliberate, are dealt with through school procedures.
6. **Child Protection Officer**
   The CPD must include in the School's Child Protection Policy the issue of 'E' Safety, and be trained and aware of appropriate strategies for dealing with breach of 'E' Safety.
7. **Pupils**
   Our pupils are responsible, and made aware of how to create a safe ICT learning environment. They must accept the responsibilities to seek help or advice if they experience any problems on-line, and the consequences of breaches.

What information are pupils given regarding the safe use of 'E' Technology?

- Pupils are given a copy of acceptable use of ICT when they join the school.
- Pupils have their own password.
- Passwords must not be shared.
- All computers have automatic updating anti-virus protection.
- Security measures are reviewed regularly, by checking content of user areas.
- Pupils are taught how to critically evaluate materials as well as learning good research skills.
- We have filtering system to prevent pupils from accessing inappropriate materials. Any breaches reported are investigated. The filtering team is contacted and the offensive site is usually removed within 24 hours.
- Pupils must report an accidental access to inappropriate materials. Deliberate access to inappropriate materials will be met with school sanctions.

- Pupils are given the understanding of 'E' Safety issues and assessed.
- Pupils are taught in ICT the dangers of technologies which they might encounter outside school.
- Pupils are reminded of Internet safety rules in all curriculum areas.
- Pupils are made aware of the impact of Cyber bullying on both the victim and the tormentor. Pupils are warned that instances of cyber bullying will be reported to the police.
- Pupils are made aware of what can be downloaded from the Internet.
- Pupils have access to Office 365 email which includes up to 5 free Microsoft Office licences to use. Use of non-school based emails will be restricted during school hours.
- Pupils are made aware of the safety issues relating to using Chat Rooms:
  - how to safely negotiate on-line relationships.
  - the importance of keeping personal information private when chatting.
  - never arrange a meeting with people who they have met on-line.
- Pupils are made aware of inappropriate activity and behaviour of using a webcam outside of school.

Website
Parents are made aware that pupils may be pictured on the website – parental consent is asked.

- **No pupils' names will be attached to images.**
- **Image files are appropriately named without using pupils' names.**
- **Images are appropriately stored on school network.**
- **Images must only be taken on school cameras.**

Access to 'E' technology for Staff
Access to the school network will be provided for you to carry out recognised school work, but only on the understanding that you agree to follow these guidelines.

General

- Users are responsible for good behaviour on the network, Internet and e-mail. General school rules apply. There is to be no eating, drinking or grooming near to equipment due to the serious damage that may be caused.
- Intentional damage to computers, computer systems or computer networks, including unauthorised damage or interference to any files is not permitted and may be considered a criminal offence under the Computer Misuse Act 1990.
- The unauthorised access or use of personal information, contrary to the provisions of the Data Protection Act and Computer Misuse Act is not permitted.
- If a "virus alert" occurs when transferring work files from a USB stick a member of the ICT staff should be informed immediately. Use of the main software packages is continually audited for each user.
- Sites visited on the Internet are also monitored.

Access to Computers

- Access to the school network is available from any network station during the normal school day.
- Staff are responsible to ensure that the computers in their classrooms and work areas are turned off at the end of the day.
- Computer equipment should not be taken off-site without formal authorisation.
- Please leave the computer and its surroundings as you would wish to find them.
- Each department is responsible for the maintenance costs of the laptops on the laptop trolleys.

Passwords

It is highly recommended that you choose a strong password that has a combination of upper and lower case letters, number and special characters or choose a group of random letters that does not make a word.

Making changes to your password should be done on a regular basis and sharing your password with a colleagues or pupils should be avoided.

Data Encryption
As a school we use data on a daily basis. This data may contain information on pupils and staff. Data that is used on external storage devices (i.e. memory sticks, external hard drive, CD etc.) should have be protected by an encrypted software and decrypted by the member of staff handling the data when needed. If the storage device gets lost or stolen then there is a protection of the encryption code that prevents access from unauthorised personnel.

File Security

- All users have their own area for storing their work on the network server hard disk (the 'My Document' folder). This means that they can access their work from any network station.
- Computer file storage areas will be treated as school property.

- ICT technicians can view a computer screen at anytime from anywhere on the school network without the user's knowledge, to ensure that the system is being used responsibly.
- The network servers are located within the computer store room. This store is out of bounds to all staff (except ICT staff) and children and is to be kept locked by the Network Manager when not under direct supervision.
- The system performs an automatic backup of each server hard disk every night. Backups are kept for thirty days and then the data is over written with new backups. Occasional backups are taken at key points (end of term, pre-upgrades, etc) are kept in the school safe for longer periods of time before reuse.
- Important work files must be copied to the OneDrive or your encrypted data-pen/stick, in case you accidentally damage them or delete them from the network server.
- It is forbidden to trespass in others' folders, work or files against Computer Misuse Act 1990.
- Users should not expect that their work and e-mails would always be private.
- Pupils' password protected files may be deleted.
- Precautions are taken to reduce the chances of infection by computer viruses via the Internet, e-mail or USB stick. The anti-virus software, which is installed on all school network stations and server, is updated regularly.
- An automatic weekly search is made for any executable program and zip files stored in pupil user areas. These are automatically logged against the user then deleted.
- Accounts not used within a full academic year will be deleted, including all work saved.
- All pupil and staff use of e-technology will be monitored and checked for any breaches in the policy.

Supervision during lessons in the ICT Suite or on the laptops

- Staff should supervise the use of the network as closely as is reasonably possible during timetabled lessons. It should be realised however, that all users do have access to the network at other times and with very little supervision beyond the restrictions contained in this policy document.
- Staff are to monitor the websites and email addresses being used in ICT based lessons and report any unsuitable websites to a member of the ICT teaching staff or ICT technicians so that they can be investigated and dealt with appropriately.
- Staff are to monitor the pupils during lesson when they are using the equipment and will report any damage to the ICT technicians. Any pupils who cause intentional damage can be sent a letter to request a contribution to the replacement of the equipment, please report to Head of ICT.
- Any disclosures by pupils of instances of cyber-bullying should be referred to Form tutor/HOS/Child Protection officer depending on the severity of the incident.

Installing and Copying Software

- The unauthorised copying of software, contrary to the provisions of the Copyright, Design and Patent Act 1988, is not permitted.
- Games must not be loaded, played or used on any computer unless approved by the Head of ICT/ICT technicians for authorised training or teaching purposes.
- It is forbidden to load executable programs from a CD-ROM or other removable media, or from the Internet. Only a member of the ICT technician staff may do this.
- The installing, copying or transmitting of obscene materials is not permitted and may be considered a criminal offence under the Obscene Publications Act 1959/1964.
- Staff are encouraged to bring laptops to school every day to ensure anti-virus and other updates are able to take place.
- Staff should not install any software onto a school laptop without speaking to the ICT technicians first.

Hardware Security

- An inventory is maintained by **Mr Wieremiewicz** of all staff laptops and PCs together with make, model, serial number and location.

- All PCs are maintained by a service contract.
- Rooms containing computers must be locked overnight.
- Those holding keys to the computer room must keep them in a secure place.
- An inventory should be maintained containing a record for each item of software that is available for use on the network and the number of licences held.
- Licences and invoices must be sent to the ICT department for filing in case proof of ownership is required.

Filtering and monitoring

- School has effective web content filtering. If when using the internet you discover inappropriate content please report to **WIM/HIL** immediately.
- School PCs and staff laptops have monitoring software on them. This software will monitor use even when your laptop is off the school site.

Usage of SIMS

Security
This section of the policy is intended to minimise security risks. These risks might affect the integrity of Saint John Wall Catholic School's data, the authorised SIMS user and the individuals to which the SIMS data pertains. In particular these risks arise from:

- The intentional or unintentional disclosure of login credentials to the SIMS system by authorised users
- The wrongful disclosure of private, sensitive and confidential information

- Exposure of the school to vicarious liability for information wrongfully disclosed by authorised users

Data Access

This section of the policy aims to ensure all relevant aspects of the Data Protection Act (1998) and Fair Processing Policy are adhered to.

This section of the policy aims to promote best use of the SIMS system to further the communication and freedom of information between Saint John Wall Catholic School and Parents/Guardians.

Authorised SIMS users

The school's SIMS system is provided for use only by persons who are legally responsible for pupil(s) currently attending the school. Access is granted only on condition that the individual formally agrees to the terms of this section of the policy.

Personal Use

Information made available through the SIMS system is confidential and protected by law under the Data Protection Act (1998). To ensure that:

- Users must not distribute or disclose any information obtained from the SIMS system to any person(s) with the exception of the pupil to which the information relates to or to other adults with parental responsibility
- Users should not attempt to access the SIMS system in any environment where the security of the information contained in the SIMS system may be placed at risk e.g. a cybercafé

Password Policy

You must assume personal responsibility for your username and password. Never use anyone else's username or password.

You must always keep your individual user name and password confidential. These usernames and passwords should ***never*** be disclosed to anyone. Passwords and usernames should never be shared.

You must change your password upon first use of the SIMS system. This is necessary to help maintain the security of the SIMS system. You ***must*** set a ***strong*** password that is not easily identifiable.

Please Note: *As soon as you have finished with SIMS you **must** log off the system. Users are liable for any potential misuse of the system and/or breach of the data protection act that may occur as a result of failing to adhere to any rules/guidelines listed in this section of the policy.*

Making changes to your password should be done on a regular basis and sharing your password with a colleagues or pupils should be avoided.

Data Encryption

As a school we use data on a daily basis. This data may contain information on pupils and staff. Data that is used on external storage devices (i.e. memory sticks, external hard drive, CD etc.) should be protected by an encrypted software and decrypted by the member of staff handling the data when needed. If the storage device gets lost or stolen then there is a protection of the encryption code that prevents access from unauthorised personnel.

Memory Sticks

- Ensure you password protect your memory stick
- Use a strong password i.e. use numbers and symbols etc.
- When using memory sticks and portable hard drives in school computers users will be asked to encrypt the drive, if user won't encrypt the drive only files on the memory stick can be accessed and nothing can be copied to the memory stick until fully encrypted
- If you lose your school memory stick you **must** inform, HAN, WIM/HIL immediately.
- OneDrive – we strongly encourage users to copy all the data to their OneDrive which is stored on Microsoft password protected cloud (part of Office 365).

Please note

Data Protection must be taken seriously. It is a legal requirement. It is your responsibility to ensure that you are entitled to have to the data or information and ensure that it is protected both on and off the school site at all times. Please keep memory sticks and other external storage devices safe and secure.

Use of Images/Videos

Images/Videos of staff or pupils of Saint John Wall should only be used in the interests of the school. Images/videos should not be shared or used outside of school context on any social network site. Never use pupil images without approval from the Headteacher and subject to parental approval. If you need any clarification on the use of images/videos you are strongly advised to discuss this with the Headteacher.

Important points to note:

- Images/videos should only be taken using official school cameras/ipads (DO NOT USE YOUR MOBILE PHONE OR ANY PERSONAL ELECTRONIC DEVICE).
- Images/videos must be passed on to ICT Technicians for safe storage on the school network.
- Do not attach pupils names to images.
- Do not store images/videos on the pupil common drive (K:).

- Images must not be given to pupils electronically or without parental consent.
- Paper files of pupil images must be shredded when no longer required. Do not dispose of them in the recycling bags or bins.
- Images on CD that are no longer required should be passed to Mr Mull for shredding.

Publications

Written consent is required from parents for any publications of pupils regarding images/videos. There is currently a media consent form which parents fill out. Please do not publicise images/videos without checking parental consent forms – **Mr Mull** has these forms and approval from the Headteacher is required for publications.

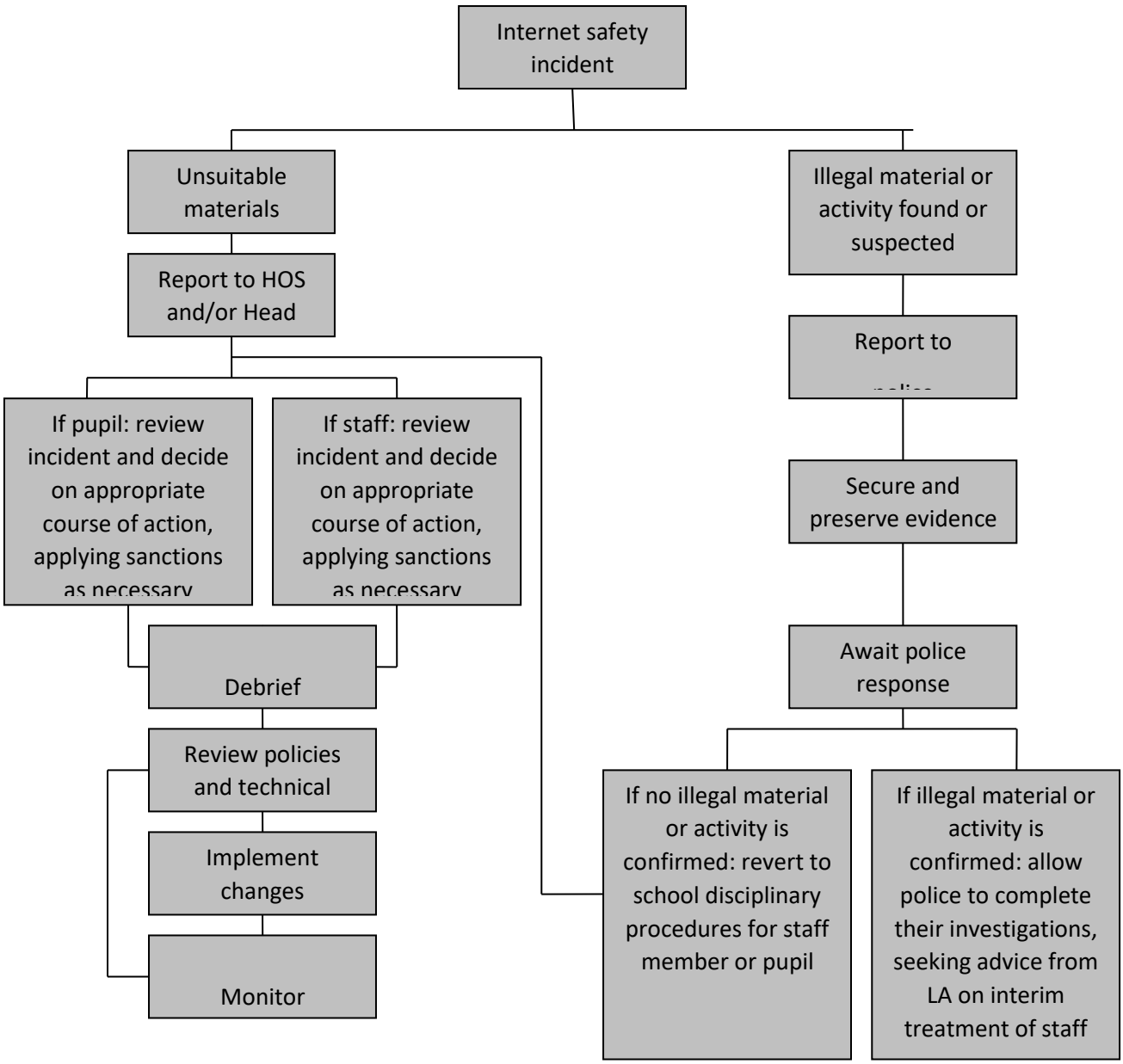
E-Mail Good Practice for Managing E-Mails

Eleven things you need to know about e-mails and sending e-mails.

1. **Email has replaced Telephone calls and memos**
   - E-mails are much quicker and faster than phone conversations. The language in an e-mail is much less formal and can be open to misinterpretation than a written memo or formal letter. E-mails should be laid out in a standard format.
2. **E-mail is not always the most secure way to send information**
   - When sending information think about how secure the e-mail is. If the e-mail ends up in the wrong hands this could lead to bad publicity in the media. If the wrong data is sent you may get in trouble from the Information Commissioner. Never send personal information (such as pupil's name) in the subject line.
3. **E-mail is disclosable under access to information rules**
   - All of the school's data is disclosable under the Freedom of Information and Data Protection acts. Anything you write in an e-mail can be made public.
4. **E-mails are not always deleted straight away**
   - E-mails can remain in the system for many years even though you may have deleted the e-mail it does not mean that the other person has. This copy of the e-mail can be disclosable under the Freedom of Information Act 2000 or the Data Protection Act 1998. **Please take into account that when you delete an e-mail in the Office 365, Microsoft will still have a copy which can be restored as far back as a couple of months and in some cases even a year.**
5. **E-mail can form a contractual obligation**
   - Agreements entered into by e-mail do form a contract. You need to be aware of this if you enter into an agreement with anyone, especially external contractors. Individual members of staff should not enter into agreements either with other members of staff internally or with external contractors unless they are authorised to do so.
6. **E-mail systems are used to store data which should be stored elsewhere.**
   - Attachments should be saved electronically or printed out and not just stored on the e-mail system. When printing out e-mails do not leave them lying around (in eg the staff room or on your desk). The content or information may be personal, confidential or include sensitive information. In addition you need to be aware that e-mails may include student's e-mails.
7. **Employers must be careful how they monitor e-mails.**
   - Employers can monitor the e-mails of its employees provided the employees have been notified.
8. **E-mail is one of the common causes of stress in the work place.**
   - The best practice is to regularly file and delete unwanted e-mails. A build-up of e-mails can cause the staff to feel that they have lost control of the situation, leading to unnecessary amounts of stress.

9. **E-Mails should not be forwarded**
    - When an e-mail is received from someone you should not forward it on to anyone unless you have had consent from the original sender. The e-mail may contain sensitive information which is only intended for you.
10. **Do not use personal e-mails**
    - The school e-mail system must be used for all professional related work. When sending in cover work to PAG or to any other member of staff, please do not use your personal e-mails. The school has an e-mail facility so please use it. If you send an e-mail using your personal e-mail and the member of staff you sent the e-mail to accidently forget to pick that e-mail off their desk or on the printer, students will have access to both your name and e-mail address.
    - Do not register into any school related services with non-school emails.
    - Do not forward school emails to your private email.
11. **Good practices**
    - Always make sure that you destroy e-mails and personal information in the correct way. For e.g use a shredder. When leaving your computer unattended always lock the computer, for the safety of both staff and students.

Flowchart for responding to Internet safety incidents in school.



Staff Agreement

All staff have a responsibility to ensure that the Internet and Email facilities are used in an appropriate fashion to support them to carry out their duties in school. The use of school resources and hardware for personal use is acceptable. However, this must not happen at a time when a colleague is involved in the execution of their professional duties. In becoming an employee of Saint John Wall all staff accept and acknowledge this policy and the principles of good professional practice and agree to the following:

- I will refrain from accessing any Newsgroups, links, list servers, web pages or other areas of cyberspace that would consider offensive I the judgement of the school's Head of School (or delegate) because of pornographic, racist, violent, illegal, illicit or other content.
- Accordingly, I am responsible for monitoring and appropriately rejecting materials, links, dialogues and information accessed/reviewed by me.
- I will report any incident where a colleague uses school equipment in an unacceptable manner which breaches any aspect or principle of the policy.
- I will not take ICT equipment home without obtaining prior permission from the Head of School (or delegate)
- The school has effective web content filtering, but not all offensive material will automatically be detected. I will not try to 'cheat' the filtering system, and search for information of an offensive nature.
- I accept responsibility to keep copyrighted material from entering the school. Therefore I will not download software, games, music, graphics, videos or text materials that are copyrighted. I will not violate any copyright laws by posting or distributing copyrighted materials.
- I will not reveal personal information, including names, addresses, credit card details and telephone numbers of others or myself.
- I will not damage computers, computer systems or networks. Furthermore, if I discover any methods of causing damage I will report them to the Head of ICT and will not demonstrate them to others.
- I will not attempt to change any computer, monitor or software settings on any school computers.
- I will abide by the current sign-on procedures for access to the computer network, respect other people's work and not attempt to access it on the network by using either alias' or passwords that are not mine.
- The entire network is protected by anti-virus software. Staff are advised to use anti-virus software on home computers and laptops. If a virus is reported on screen, a member of ICT staff should be informed immediately.
- The Network Manager carries out daily network backups. I will, however, attempt to save my own work correctly and use sensible file management techniques at all times
- I will not take digital photographs, or edit digital images of staff or pupils without their consent
- I will password protect and take responsibility of all data held on my usb storage devices. I will also take care of the usb memory stick provided to me by the school.
- If I violate any of the terms of this agreement, I will be denied access of the Internet and/or computers for a time to be determined by the Head of School and may face further disciplinary action.

Mobile Technologies Policy (inc. BYOD/BYOT)

Mobile technology devices may be a school owned/provided or privately owned smartphone, tablet, notebook / laptop or other technology that usually has the capability of utilising the school's wireless network. The device then has access to the wider internet which may include the school's learning platform and other cloud based services such as email and data storage.

The absolute key to considering the use of mobile technologies is that the pupils / students, staff and wider school community understand that the primary purpose of having their personal device at school is educational and that this is irrespective of whether the device is school owned/provided or personally owned. The mobile technologies policy should sit alongside a range of polices including but not limited to the Safeguarding Policy, Bullying Policy, Acceptable Use Policy, policies around theft or malicious damage and the Behaviour Policy. Teaching about the safe and appropriate use of mobile technologies should be included in the online safety education programme.

Potential Benefits of Mobile Technologies

Research has highlighted the widespread uptake of mobile technologies amongst adults and children of all ages. Web-based tools and resources have changed the landscape of learning. Students now have at their fingertips unlimited access to digital content, resources, experts, databases and communities of interest. By effectively maximizing the use of such resources, schools not only have the opportunity to deepen student learning, but they can also develop digital literacy, fluency and citizenship in students that will prepare them for the high tech world in which they will live, learn and work.

For further reading, please refer to "Bring your own device: a guide for schools" by Alberta Education available at: http://education.alberta.ca/admin/technology/research.aspx and to the "NEN Technical Strategy Guidance Note 5 – Bring your own device" - http://www.nen.gov.uk/bring-your-own-device-byod/

Considerations

There are a number of issues and risks to consider when implementing mobile technologies, these include; security risks in allowing connections to your school network, filtering of personal devices, breakages and insurance, access to devices for all students, avoiding potential classroom distraction, network connection speeds, types of devices, charging facilities, total cost of ownership

Schools may consider implementing the use of mobile technologies as a means of reducing expenditure on school provided devices. However, it is important to remember that the increased network management costs and overheads involved in implementing this properly are likely to counterbalance or outweigh any savings.

The use of mobile technologies brings both real benefits and challenges for the whole school community – including teachers - and the only effective way for a school to implement these successfully is to involve the whole school community from the outset. Before the school embarks on this path, the risks and benefits must be clearly identified and shared with all stakeholders.

A range of mobile technology implementations is possible. School should consider the following statements and remove those that do not apply to their planned implementation approach.

- The school Acceptable Use Agreements for staff, pupils/students and parents/carers will give consideration to the use of mobile technologies
- The school allows: (the school should complete the table below to indicate which devices are allowed and define their access to school systems)

	School Devices			*Personal Devices*		
	School owned and allocated to a single user	School owned for use by multiple users	Authorised device[1]	Pupil/Student owned	Staff owned	Visitor owned
Allowed in school	**Yes**	**Yes**	**Yes**	Yes / No[2]	Yes/ No[2]	Yes/ No[2]
Full network access	*Yes*	*Yes*	*Yes*			
Internet only						
No network access						

[1] Authorised device – purchased by the pupil/family through a school-organised scheme. This device may be given full access to the network as if it were owned by the school

[2] The school should add below any specific requirements about the use of personal devices in school, e.g. storing in a secure location, use during the school day, liability, taking images etc

- **The school has provided technical solutions for the safe use of mobile technology for school devices/personal devices (delete / amend as appropriate):**
  - **All school devices are controlled though the use of Mobile Device Management software**
  - **Appropriate access control is applied to all mobile devices according to the requirements of the user (e.g Internet only access, network access allowed, shared folder network access)**
  - **The school has addressed broadband performance and capacity to ensure that core educational and administrative activities are not negatively affected by the increase in the number of connected devices**
  - **For all mobile technologies, filtering will be applied to the internet connection and attempts to bypass this are not permitted**
  - **Appropriate exit processes are implemented for devices no longer used at a school location or by an authorised user. These may include; revoking the link between MDM software and the device, removing proxy settings, ensuring no sensitive data is removed from the network, uninstalling school-licenced software etc.**
  - *All school devices are subject to routine monitoring*
  - *Pro-active monitoring has been implemented to monitor activity*
- *When personal devices are permitted:*
  - *All personal devices are restricted through the implementation of technical solutions that provide appropriate levels of network access*
  - *Personal devices are brought into the school entirely at the risk of the owner and the decision to bring the device in to the school lies with the user (and their parents/carers) as does the liability for any loss or damage resulting from the use of the device in school*
  - *The school accepts no responsibility or liability in respect of lost, stolen or damaged devices while at school or on activities organised or undertaken by the school (the school recommends insurance is purchased to cover that device whilst out of the home)*
  - *The school accepts no responsibility for any malfunction of a device due to changes made to the device while on the school network or whilst resolving any connectivity issues*

- *The school recommends that the devices are made easily identifiable and have a protective case to help secure them as the devices are moved around the school. Pass-codes or PINs should be set on personal devices to aid security*
- *The school is not responsible for the day to day maintenance or upkeep of the users personal device such as the charging of any device, the installation of software updates or the resolution of hardware issues*

- **Users are expected to act responsibly, safely and respectfully in line with current Acceptable Use Agreements, in addition;**
  - **Devices may not be used in tests or exams**
  - **Visitors should be provided with information about how and when they are permitted to use mobile technology in line with local safeguarding arrangements**
  - **Users are responsible for keeping their device up to date through software, security and app updates. The device is virus protected and should not be capable of passing on infections to the network**
  - **Users are responsible for charging their own devices and for protecting and looking after their devices while in school**
  - **Personal devices should be charged before being brought to school as the charging of personal devices is not permitted during the school day**
  - **Devices must be in silent mode on the school site and on school buses**
  - **School devices are provided to support learning. It is expected that pupils/students will bring devices to school as required.**
  - **Confiscation and searching (England) - the school has the right to take, examine and search any device that is suspected of unauthorised use, either technical or inappropriate.**
  - **The changing of settings (exceptions include personal settings such as font size, brightness, etc…) that would stop the device working as it was originally set up and intended to work is not permitted**
  - **The software / apps originally installed by the school must remain on the school owned device in usable condition and be easily accessible at all times. From time to time the school may add software applications for use in a particular lesson. Periodic checks of devices will be made to ensure that users have not removed required apps**
  - **The school will ensure that school devices contain the necessary apps for school work. Apps added by the school will remain the property of the school and will not be accessible to students on authorised devices once they leave the school roll. Any apps bought by the user on their own account will remain theirs.**
  - **Users should be mindful of the age limits for app purchases and use and should ensure they read the terms and conditions before use.**
  - **Users must only photograph people with their permission. Users must only take pictures or videos that are required for a task or activity. All unnecessary images or videos will be deleted immediately**
  - *Devices may be used in lessons in accordance with teacher direction*
  - *Staff owned devices should not be used for personal purposes during teaching sessions, unless in exceptional circumstances*
  - *Printing from personal devices will not be possible*

Social Media

Social media (e.g. Facebook, Twitter, LinkedIn) is a broad term for any kind of online platform which enables people to directly interact with each other. However some games, for example Minecraft or World of Warcraft and video sharing platforms such as You Tube have social media elements to them.

The school recognises the numerous benefits and opportunities which a social media presence offers. Staff, parents/carers and pupils/students are actively encouraged to find creative ways to use social media. However, there are some risks associated with social media use, especially around the issues

of safeguarding, bullying and personal reputation. This policy aims to encourage the safe use of social media by *the school*, its staff, parents, carers and children.

Scope

This policy is subject to the school's Codes of Conduct and Acceptable Use Agreements.
This policy:

- Applies to all staff and to all online communications which directly or indirectly, represent the school.
- Applies to such online communications posted at any time and from anywhere.
- Encourages the safe and responsible use of social media through training and education
- Defines the monitoring of public social media activity pertaining to the school

The school respects privacy and understands that staff and pupils/students may use social media forums in their private lives. However, personal communications likely to have a negative impact on professional standards and/or the school's reputation are within the scope of this policy.

Professional communications are those made through official channels, posted on a school account or using the school name. All professional communications are within the scope of this policy.

Personal communications are those made via a personal social media accounts. In all cases, where a personal account is used which associates itself with the school or impacts on the school, it must be made clear that the member of staff is not communicating on behalf of the school with an appropriate disclaimer. Such personal communications are within the scope of this policy.

Personal communications which do not refer to or impact upon the school are outside the scope of this policy.

Digital communications with pupils/students are also considered. *Staff may use social media to communicate with learners via a school social media account for teaching and learning purposes but must consider whether this is appropriate and consider the potential implications.*

Organisational control

Roles & Responsibilities

- **SLT**
  - Facilitating training and guidance on Social Media use.
  - Developing and implementing the Social Media policy
  - Taking a lead role in investigating any reported incidents.
  - Making an initial assessment when an incident is reported and involving appropriate staff and external agencies as required.
  - Receive completed applications for Social Media accounts
  - Approve account creation

- **Administrator / Moderator**
  - Create the account following SLT approval
  - Store account details, including passwords securely
  - Be involved in monitoring and contributing to the account
  - Control the process for managing an account after the lead staff member has left the organisation (closing or transferring)
- **Staff**
  - Know the contents of and ensure that any use of social media is carried out in line with this and other relevant policies
  - Attending appropriate training
  - Regularly monitoring, updating and managing content he/she has posted via school accounts

- Adding an appropriate disclaimer to personal accounts when naming the school

Process for creating new accounts

The school community is encouraged to consider if a social media account will help them in their work, e.g. a history department Twitter account, or a "Friends of the school" Facebook page. Anyone wishing to create such an account must present a business case to the School Leadership Team which covers the following points:-

- The aim of the account
- The intended audience
- How the account will be promoted
- Who will run the account (at least two staff members should be named)
- Will the account be open or private/closed

Following consideration by the SLT an application will be approved or rejected. In all cases, the SLT must be satisfied that anyone running a social media account on behalf of the school has read and understood this policy and received appropriate training. This also applies to anyone who is not directly employed by the school, including volunteers or parents.

Monitoring

School accounts must be monitored regularly and frequently (preferably 7 days a week, including during holidays). Any comments, queries or complaints made through those accounts must be responded to within 24 hours (or on the next working day if received at a weekend) even if the response is only to acknowledge receipt. Regular monitoring and intervention is essential in case a situation arises where bullying or any other inappropriate behaviour arises on a school social media account.

Behaviour

- **The school requires that all users using social media adhere to the standard of behaviour as set out in this policy and other relevant policies.**
- **Digital communications by staff must be professional and respectful at all times and in accordance with this policy**. Staff will not use social media to infringe on the rights and privacy of others or make ill-considered comments or judgments about staff. School social media accounts must not be used for personal gain. Staff must ensure that confidentiality is maintained on social media even after they leave the employment of the school.
- Users must declare who they are in social media posts or accounts. Anonymous posts are discouraged in relation to school activity.
- If a journalist makes contact about posts made using social media staff must follow the school media policy before responding.
- Unacceptable conduct, (e.g. defamatory, discriminatory, offensive, harassing content or a breach of data protection, confidentiality, copyright) will be considered extremely seriously by the school and will be reported as soon as possible to a relevant senior member of staff, and escalated where appropriate.
- The use of social media by staff while at work may be monitored, in line with school policies. *The school permits reasonable and appropriate access to private social media sites. However, where excessive use is suspected, and considered to be interfering with relevant duties, disciplinary action may be taken*
- The school will take appropriate action in the event of breaches of the social media policy. Where conduct is found to be unacceptable, the school will deal with the matter internally. Where conduct is considered illegal, the school will report the matter to the police and other relevant external agencies, and may take action according to the disciplinary policy.

Legal considerations

- **Users of social media should consider the copyright of the content they are sharing and, where necessary, should seek permission from the copyright holder before sharing.**
- **Users must ensure that their use of social media does not infringe upon relevant data protection laws, or breach confidentiality.**

Handling abuse

- When acting on behalf of the school, handle offensive comments swiftly and with sensitivity.
- If a conversation turns and becomes offensive or unacceptable, school users should block, report or delete other users or their comments/posts and should inform the audience exactly why the action was taken
- If you feel that you or someone else is subject to abuse by colleagues through use of a social networking site, then this action must be reported using the agreed school protocols.

Tone

The tone of content published on social media should be appropriate to the audience, whilst retaining appropriate levels of professional standards. Key words to consider when composing messages are:

- Engaging
- Conversational
- Informative
- Friendly (on certain platforms, e.g. Facebook)

Use of images

School use of images can be assumed to be acceptable, providing the following guidelines are strictly adhered to.

- **Permission to use any photos or video recordings should be sought in line with the school's digital and video images policy**. If anyone, for any reason, asks not to be filmed or photographed then their wishes should be respected.
- **Under no circumstances should staff share or upload student pictures online other than via school owned social media accounts**
- Staff should exercise their professional judgement about whether an image is appropriate to share on school social media accounts. Students should be appropriately dressed, not be subject to ridicule and must not be on any school list of children whose images must not be published.
- If a member of staff inadvertently takes a compromising picture which could be misconstrued or misused, they must delete it immediately.

Personal use

- **Staff**
    - Personal communications are those made via a personal social media accounts. In all cases, where a personal account is used which associates itself with the school or impacts on the school, it must be made clear that the member of staff is not communicating on behalf of the school with an appropriate disclaimer. Such personal communications are within the scope of this policy.
    - Personal communications which do not refer to or impact upon the school are outside the scope of this policy.
    - Where excessive personal use of social media in school is suspected, and considered to be interfering with relevant duties, disciplinary action may be taken
    - *The school permits reasonable and appropriate access to private social media sites.*

- **Pupil/Students**
    - **Staff are not permitted to follow or engage with current or prior pupils/students of the school on any personal social media network account.**
    - The school's education programme should enable the pupils/students to be safe and responsible users of social media.
    - Pupils/students are encouraged to comment or post appropriately about the school. Any offensive or inappropriate comments will be resolved by the use of the school's behaviour policy
- **Parents/Carers**
    - **If parents/carers have access to a school learning platform where posting or commenting is enabled, parents/carers will be informed about acceptable use.**
    - The school has an active parent/carer education programme which supports the safe and positive use of social media. This includes information on the website.
    - Parents/Carers are encouraged to comment or post appropriately about the school. In the event of any offensive or inappropriate comments being made, the school will ask the parent/carer to remove the post and invite them to discuss the issues in person. If necessary, refer parents to the school's complaints procedures.

Monitoring posts about the school

- As part of active social media engagement, it is considered good practice to pro-actively monitor the Internet for public postings about the school.
- The school should effectively respond to social media comments made by others according to a defined policy or process.

Appendix

Managing your personal use of Social Media:

- "Nothing" on social media is truly private
- Social media can blur the lines between your professional and private life. Don't use the school logo and/or branding on personal accounts
- Check your settings regularly and test your privacy
- Keep an eye on your digital footprint
- Keep your personal information private
- Regularly review your connections – keep them to those you want to be connected to
- When posting online consider; Scale, Audience and Permanency of what you post
- If you want to criticise, do it politely.
- Take control of your images – do you want to be tagged in an image? What would children or parents say about you if they could see your images?
- Know how to report a problem

Managing school social media accounts

The Do's

- Check with a senior leader before publishing content that may have controversial implications for the school
- Use a disclaimer when expressing personal views
- Make it clear who is posting content
- Use an appropriate and professional tone
- Be respectful to all parties
- Ensure you have permission to 'share' other peoples' materials and acknowledge the author
- Express opinions but do so in a balanced and measured manner
- Think before responding to comments and, when in doubt, get a second opinion
- Seek advice and report any mistakes using the school's reporting process
- Consider turning off tagging people in images where possible

The Don'ts

- Don't make comments, post content or link to materials that will bring the school into disrepute
- Don't publish confidential or commercially sensitive material
- Don't breach copyright, data protection or other relevant legislation
- Consider the appropriateness of content for any audience of school accounts, and don't link to, embed or add potentially inappropriate content
- Don't post derogatory, defamatory, offensive, harassing or discriminatory content
- Don't use social media to air internal grievances

STAFF E-SAFETY AGREEMENT

Staff Name:_____

I acknowledge receipt of the staff E-Safety policy & agreement and agree to abide by its terms and conditions.

Signed:_____ Date:_____/_____/_____

Please complete & return to **Mariusz Wieremiewicz**

Appendix 2
Internet and Electronic Mail Policy

All our pupils are given opportunity to have their own e-mail address and access to the Internet outside of school time. For the pupils to benefit from this facility we need your consent. It is therefore very important that you read and understand this letter before completing and returning the attached form to the school. Once we have received it your child will be given their e-mail address and a card allowing them to attend after school computer sessions when run.

Our Internet access is provided through RM Education, and filtering/monitoring is provided by Smoothwall. Email is provided by Microsoft, each pupil is entitled to 5 free Office 2016 licenses (desktop, phone, tablet, iOS) and 1TB of online storage.

Access to e-mail and the Internet will enable students to explore thousands of libraries, databases and bulletin boards and to exchange messages with Internet users throughout the world. Parents and guardians should be warned that some material accessible via the Internet might contain items that are illegal, defamatory, inaccurate or potentially offensive to some people. Our filtering provider Smoothwall offers a service, which filters out the known unpleasant material. However, although our intent is to make Internet access available in order to further our education goals and objectives, students may find ways to access other materials as well. We believe that the benefits to students from access to the Internet exceed any disadvantages. Ultimately, parents and guardians of students are responsible for setting and conveying standards that their children should follow when using media and information sources. To that end we support and respect each family's right to decide whether or not to apply for access.

The school has a principle of access to certain computer facilities during breaks, lunchtimes and occasionally after school. It is impossible to monitor all pupils' access at all times, we shall therefore, have to depend upon four things in order to ensure appropriate access to and behaviour on the Internet:

- the natural honesty of most children,
- the ultimate parental responsibility for their children's behaviour,
- the ability of the computer network to record details of a pupil's Internet access
- and the threat of very restricted computer access, in addition to other disciplinary action, following inappropriate behaviour over the Internet.

Staff will provide guidance to students as they make use of telecommunications and electronic information sources to conduct research and other studies related to the curriculum. All students will be informed by staff of their rights and responsibilities as users of the network, prior to gaining access to that network, either as an individual user or as a member of a glass or group. As much as possible, students will be directed to information resources that have been reviewed and evaluated by staff at the school. Students should not bring memory sticks or CD's to school unless they have permission from a member of the ICT Department and the disks are checked for viruses before use in the school computers.

Saint John Wall Catholic School

A Catholic School For All

Mission Statement

'To educate each and every unique child in our care to hear and respond to what God calls them

ACCEPTABLE USE OF E-TECHNOLOGIES
PUPIL POLICY

When I am using computer or other technologies, I want to feel safe all the time.

I agree that I will:

- Always keep my passwords secret
- Not attempt to gain unauthorised access to the school network or to any other computer system accessible via the Internet.
- Not attempt to log on using another person's username and password with or without their permission.
- Not attempt to access another person's files.
- Only visit sites which are appropriate to my work at the time.
- Tell a responsible adult straight away if anything makes me feel scared or uncomfortable online.
- Not visit websites that contain unsuitable, obscene or offensive material. If I am unsure if a site is suitable, I will ask a member of staff.
- Make sure all messages I send are respectful.
- Show a responsible adult if I get a nasty message or get sent anything that makes me feel uncomfortable.
- Not reply to any nasty message or anything which makes me feel uncomfortable.
- Only email people I know or those approved by a responsible adult.
- Only use email accounts that have been provided by school, use of personal email accounts will be restricted during school hours (Hotmail or Yahoo).
- Not use offensive or threatening language in my e-mails or in any other communication on the Internet.
- Always keep my personal details private (my name, family information, journey to school, my pets and hobbies are all examples of personal details).
- Only copy pictures or text into my area on the network. I will not download any other type of file (for example software, games, screen savers, etc.).
- Not copy or make use of any material without giving credit to the author otherwise I will be breaking the law on copyright.
- Not take information from the Internet and pass it off as my own work (this is known as plagiarism).
- Not undertake financial transactions on behalf of the school.
- Report any misuse of the Internet/network immediately to a member of staff.
- Not intentionally waste limited resources such as printer paper and toner.
- Not download games/videos/music.
- Not remove picture/files from the school network for social networking websites.
- Will not remove video files for internet use.

I understand the school will:

- Conduct regular monitoring of the Internet use
- Report incidents to the E-Safety co-ordinator, which will be recorded on my school file and if necessary parents will be informed.
- My network privileges will be removed if I fail to adhere to the use of the E-technologies policy.

Print Name: _____

Signature: _____ Date: _____/_____/_____

Ratified by Governors: 07/07/2021
Next Review Due: 07/07/2022
(This policy will remain in force beyond the review date if no updates are required)