



St. Nicholas Catholic Primary School



Policy on Online Safety

Policy Written & Agreed:

Ratified by Full Governing Body:

To be reviewed:

September 2026

September 2027



St. Nicholas

Whole School Policy on Online Safety

This Online Safety policy:-

- is based on DfE Teaching Online Safety in Schools guidance – January 2023
- follows Keeping Children Safe in Education guidance – September 2026
- reflects the consensus of opinion of the whole staff;
- was discussed, written and agreed by the whole staff;
- has been approved by the Governing body.

The implementation and ownership of this policy is the responsibility of the whole staff.

The overall accountability and effectiveness of the policy will be the responsibility of the Executive Head Teacher and Senior Leadership Team.

At St. Nicholas Catholic Primary School, we take a professional and pro-active approach to Online Safety and we are committed to keeping our children safe both in and out of School. As a Catholic school, we believe all are created in the image and likeness of God and should be protected from harm of any description.

1.0 INTRODUCTION

- 1.1 It is essential that children are safeguarded from potentially harmful and inappropriate online material. An effective whole school and college approach to online safety empowers us to protect and educate our pupils, students and staff in their use of technology and establishes mechanisms to identify, intervene in and escalate any concerns where appropriate.
- 1.2 At St. Nicholas, we understand that computer technology is an essential resource for supporting teaching and learning. The internet, and other digital and information technologies, open up opportunities for pupils and play an important role in their everyday lives.
- 1.3 Whilst we recognise the importance of promoting the use of computer technology throughout the curriculum, we also recognise the need for safe internet access and appropriate use. Our school has created this policy with the aim of ensuring appropriate and safe use of the internet and other digital technology devices by all pupils and staff.
- 1.4 The school is committed to providing a safe learning and teaching environment for all pupils and staff, and has implemented important controls to prevent any harmful risks. This policy will operate in conjunction with other important policies in our school, including our 'Anti-bullying Policy', 'General Data Protection Regulations Policy', 'Safeguarding & Child Protection Policy' and 'Acceptable Use of the Internet & Technology Policy'.
- 1.5 The breadth of issues classified within online safety is considerable and ever evolving, but can be categorised into four areas of risk (**The 4 C's**):
 - 1.5.1 **content:** being exposed to illegal, inappropriate, or harmful content, for example: pornography, fake news, racism, misogyny, self-harm, suicide, anti-Semitism, radicalisation, and extremism.
 - 1.5.2 **contact:** being subjected to harmful online interaction with other users; for example: peer to peer pressure, commercial advertising and adults posing as children or young adults with the intention to groom or exploit them for sexual, criminal, financial or other purposes.
 - 1.5.3 **conduct:** online behaviour that increases the likelihood of, or causes, harm; for example, making, sending and receiving explicit images (e.g. consensual and non-consensual sharing of nudes and semi-nudes and/or pornography, sharing other explicit images and online bullying), and
 - 1.5.4 **commerce:** risks such as online gambling, inappropriate advertising, phishing and or financial scams. If you feel your pupils, students or staff are at risk, please report it to the Anti-Phishing Working Group (<https://apwg.org/>).

2.0 USE OF THE INTERNET

- 2.1 The school understands that using the internet is important when raising educational standards, promoting pupil achievement and enhancing teaching and learning.
- 2.2 Internet use is embedded in the statutory curriculum and is therefore entitled to all pupils, though there are a number of controls required for schools to implement, which minimise harmful risks.

2.3 When accessing the internet, individuals are especially vulnerable to a number of risks which may be physically and emotionally harmful. These risks include:

- Access to illegal, harmful or inappropriate images
- Cyber bullying
- Access to, or loss of, personal information
- Access to unsuitable online videos or games
- Loss of personal images
- Inappropriate communication with others
- Illegal downloading of files
- Plagiarism and copyright infringement
- Sharing the personal information of others without the individual's consent or knowledge

3.0 ROLES & RESPONSIBILITIES

- 3.1 It is the responsibility of all staff to be alert to possible harm to pupils or staff, due to inappropriate internet access or use both inside and outside of the school, and to deal with incidents of such as a priority.
- 3.2 The Executive Head Teacher/Head Teacher/Head of School, supported by St. John Paul II Multi Academy IT Team, is responsible for ensuring the day-to-day online safety in our school, and managing any issues. The Executive Head Teacher/Head Teacher/Head of School is responsible for ensuring that any relevant staff receive continuous professional development to allow them to fulfil their role effectively.
- 3.3 The Computing Curriculum Leader will provide all relevant training and advice for members of staff on online safety.
- 3.4 The Executive Head Teacher/Head Teacher/Head of School will ensure there is a system in place which monitors online safety in the school. The Computing Curriculum Leader will regularly monitor the provision and teaching of online safety in the school and report on this to the Senior Leadership Team. The school will establish a procedure for reporting incidents and inappropriate internet use, either by pupils or staff and ensure that all members of staff are aware of the procedure when reporting online safety incidents, and will keep a log of all incidents recorded.
- 3.5 Cyber bullying incidents will be reported in accordance with the school's Anti-Bullying Policy and Behaviour Policy.
- 3.6 The Local Governing Body will hold regular meetings with the Executive Head Teacher/Head Teacher/Head of School to discuss the effectiveness of the online safety provision, current issues, and to review incident logs. The Executive Head Teacher/Head Teacher/Head of School and Local Governing Body will evaluate and review this Online Safety Policy on an annual basis, taking into account new legislation and government guidance, and previously reported incidents to improve procedures.
- 3.7 Teachers are responsible for ensuring that online safety teaching is embedded in the curriculum and safe internet access is promoted at all times. All staff are responsible for ensuring they are up-to-date with current online safety issues, and this Online Safety Policy.
- 3.8 All staff and pupils will ensure they understand and adhere to the 'Acceptable Use of the Internet Policy', which they must read and sign as part of their 'Code of Conduct' on EVERY.
- 3.9 Parents/carers are responsible for ensuring their child understands how to use computer technology and other digital devices, appropriately. The Executive Head Teacher/Head Teacher/Head of School is responsible for communicating with parents regularly and updating them on current online safety issues and control measures.

4.0 ONLINE SAFETY CONTROL MEASURES

4.1 Educating pupils:

- An online safety programme will be established and taught across the curriculum on a regular basis, ensuring pupils are aware of the safe use of new technology both inside and outside of the school.
- Pupils will be taught about the importance of online safety and are encouraged to be critically aware of the content they access online.
- Pupils will be taught to acknowledge information they access online, in order to avoid copyright infringement and/or plagiarism.
- Clear guidance on the rules of internet use will be presented in all classrooms.
- Pupils are instructed to report any suspicious use of the internet and digital devices to their teacher.

4.2 Educating staff:

- All staff will undergo online safety training on a termly basis to ensure they are aware of current online safety issues and any changes to the provision of online safety.
- All staff will undergo regular audits by the Computing Leader in order to identify areas of training need.
- All staff will employ methods of good practice and act as role models for pupils when using the internet and other digital devices.
- Any new staff are required to undergo online safety training as part of their induction programme, ensuring they fully understand this Online Safety Policy.

4.3 Internet access:

- Internet access will be authorised once parents and pupils have completed the signed consent form as part of the Acceptable Use of the Internet Policy.
- A record will be kept by the school office of all pupils who have been granted internet access.
- All users will be provided with usernames and passwords, and are advised to keep this confidential to avoid any other pupils using their login details.
- Pupils' activity is monitored by the school system **SMOOTHWALL** alerts to the Senior Leadership Team.
- Management systems will be in place to allow teachers and members of staff to control workstations and monitor pupils' activity.
- Effective filtering systems will be established to eradicate any potential risks to pupils through access to particular websites through **SMOOTHWALL via Advanced IT**.
- Any requests by staff for websites to be added or removed from the filtering list must be first authorised by the Executive Head Teacher/Head Teacher/Head of School.
- All school systems will be protected by up-to-date virus software.
- An agreed procedure will be in place for the provision of temporary users, e.g. volunteers.
- The master users' passwords is controlled by the Academy Central IT Team for security.

4.4 E-mail:

The school e-mail system is provided, filtered and monitored by St. John Paul II Multi Academy IT Team and is governed by a centralised E-mail Use Policy:

- Pupils and staff will be given approved email accounts and are only able to use these accounts.
- Use of personal e-mail to send and receive personal data or information is prohibited.
- No sensitive personal data shall be sent to any other pupils, staff or third parties via email.
- Any emails sent by pupils to external organisations will be overseen by their class teacher and must be authorised before sending.
- Chain letters, spam and all other emails from unknown sources will be deleted without opening.

4.5 Social Networking:

- Access to social networking sites will be filtered as appropriate.
- Any authorised access to social networking sites will be monitored and controlled by staff at all times and must be first authorised by the Executive Head Teacher/Head Teacher/Head of School.
- Pupils are regularly educated on the implications of posting personal data online, outside of the school.
- Staff are regularly educated on posting inappropriate photos or information online, which may potentially affect their position and the school/academy as a whole.
- Staff are not permitted to communicate with pupils over social networking sites.

4.6 Published content on the school website and images:

- The Executive Head Teacher/Head Teacher/Head of School will be responsible for the overall content of the website, and will ensure the content is appropriate and accurate.
- All contact details on the school website will be the phone, email and address of the school. No personal details of staff or pupils will be published.
- Images and full names of pupils, or any content that may easily identify a pupil, will be selected carefully, and will not be posted until authorisation from parents has been received.
- Pupils are not permitted to take or publish photos of others without permission from the individual.
- Staff are able to take images, though they must do so in accordance with school policies in terms of the sharing and distribution of such. Staff will not take images using their personal equipment.

4.7 Mobile devices:

- The Executive Head Teacher/Head Teacher/Head of School may authorise the use of mobile devices by a pupil where it is seen to be for safety or precautionary use.
- Personal mobile devices are not permitted to be used in the classroom by pupils or members of staff.
- The sending of inappropriate messages or images from mobile devices is prohibited.
- Personal mobile devices must not be used to take images of pupils or staff.
- The school will be especially alert to instances of cyber bullying and will treat such instances as a matter of high priority following the school Anti-Bullying Policy and Behaviour Policy.

4.8 Digital Media:

We respect the privacy of the school community and will obtain written permission from staff, parents, carers or pupils before any images or video are published or distributed outside the school.

- Photographs will be published in-line with the Child Protection Act and not identify any individual pupil.
- Students' full names will not be published outside the school environment.
- Permission will be obtained from parents or carers prior to pupils taking part in external video activities.

5.0 SECURITY

5.1 The school endeavours to provide a safe environment for the whole community and we review both physical and network security regularly and monitor who has access to the system.

5.2 Anti-virus software is installed on all computers and updated regularly.

5.3 Central filtering is provided and managed by Advanced IT through **SMOOTHWALL**. All staff, students, visitors, supply teachers are made aware of this and understand that if an inappropriate site is discovered it must be reported to the Executive Head Teacher/Head Teacher/Head of School who will report it to the St. John Paul II Multi Academy IT Team to be blocked. All incidents are recorded in the Online Safety log for audit purposes.

5.4 Requests for changes to the filtering will be directed to the Computing Curriculum Leader in the first instance who will forward these on to St. John Paul II Multi Academy IT Team or liaise with the Executive Head Teacher/Head Teacher/Head of School as appropriate. Change requests are recorded in the Online Safety log for audit purposes.

5.5 The school uses **SMOOTHWALL** on all school owned equipment to ensure compliance with the Acceptable Use Policies.

- Pupils use is monitored by the Computing Curriculum Leader.
- Staff use is monitored by the Executive Head Teacher/Head Teacher/Head of School.

5.6 All staff, visitors and supply teachers are issued with their own username and password for network access.

5.7 All pupils are issued with their own username and password and understand that this must not be shared.

6.0 CYBER-BULLYING

- 6.1 For the purpose of this policy, “cyber bullying” is a form of bullying whereby an individual is the victim of harmful or offensive posting of information or images, online.
- 6.2 The school recognises that both staff and pupils may experience cyber bullying and will commit to preventing any instances that should occur.
- 6.3 The school will regularly educate staff, pupils and parents on the importance of staying safe online, as well as being considerate to what they post online.
- 6.4 The school will commit to creating a learning and teaching environment which is free from harassment and bullying, ensuring the happiness of all members of staff and pupils.
- 6.5 The school has zero tolerance for cyber bullying, and any incidents will be treated with the upmost seriousness and will be dealt with in accordance with our Anti-Bullying Policy and Behaviour Policy.
- 6.6 The Executive Head Teacher/Head Teacher/Head of School will decide whether it is appropriate to notify the police of the action taken against a pupil.

7.0 REPORTING MISUSE

Misuse by pupils:

- Teachers have the power to discipline pupils who engage in misbehaviour with regards to internet use.
- Any instances of misuse should be immediately reported to a member of staff, who will then report this to the Executive Head Teacher/Head Teacher/Head of School.
- Any pupil who does not adhere to the rules outlined in our Acceptable Use of the Internet Policy and is found to be wilfully misusing the internet, will have a letter sent to their parents/carers explaining the reason for suspending their internet use.
- Members of staff may decide to issue other forms of disciplinary action to a pupil upon the misuse of the internet. This will be discussed with the Executive Head Teacher/Head Teacher/Head of School and will be issued once the pupil is on the school premises.
- Complaints of a child protection/safeguarding nature shall be dealt with in accordance with our ‘Safeguarding and Child Protection Policy’.

Misuse by staff:

- Any misuse of the internet by a member of staff should be immediately reported to the Executive Head Teacher/Head Teacher/Head of School.
- The Executive Head Teacher/Head Teacher/Head of School will deal with such incidents in accordance with the Allegations Against Staff section of our ‘Safeguarding and Child Protection Policy’, and may decide to take disciplinary action against the member of staff.
- The Executive Head Teacher/Head Teacher/Head of School will decide whether it is appropriate to notify the police or CEO of the Academy of the action taken against a member of staff.

Policy Written & Agreed:
Ratified by Full Governing Body:
To be reviewed:



 September 2026

 September 2027
