CARDINAL NEWMAN CATHOLIC SCHOOL

Online Safety Policy

Dated: July 2024

Date: Summer 2025

Mission Statement: "Knowledge through the light of faith"

Our mission is to ensure that Jesus Christ is made known to all our students by placing Christ and the teachings of the Catholic Church at the centre of all our students' lives. We endeavour to make known to every student, that they are 'Made for Greatness' because they are a child of God and are uniquely created and loved by God.

Every child is called to live out the gospel values by loving God, others and themselves and by being prepared to always do their best and be the best person they can be. Our core values (ASPIRE) are lived out within our school, to ensure that we are an active community of God.

Cardinal Newman Catholic School works with children and families as part of its activities. Our online safety policy is intended to help consider all current and relevant issues, in a whole school context, linking with other relevant policies such as the Child Protection & Safeguarding Policy 2024-2025 etc and the Prevent Policy.

The purpose of this policy statement is to:

- Ensure the safety and wellbeing of children and young people is paramount when adults, young people or children are using the internet, social media or mobile devices
- Provide staff and volunteers with the overarching principles that guide our approach to online safety
- Ensure that, as an organisation, we operate in line with our values and within the law in terms of how we use online devices.

Legal framework

This policy has been drawn up on the basis of legislation, policy and guidance that seeks to protect children in England.

Summaries of the key legislation and guidance are available on:

- online abuse
- bullying
- child protection.

We believe that:

- children and young people should never experience abuse of any kind
- children should be able to use the internet for education and personal development, but safeguards need to be in place to ensure they are kept safe at all times.

We recognise that:

- the online world provides everyone with many opportunities; however, it can also present risks and challenges
- we have a duty to ensure that all children, young people and adults involved in our organisation are protected from potential harm online
- we have a responsibility to help keep children and young people safe online, whether or not they are using Cardinal Newman Catholic School's network and devices
- working in partnership with children, young people, their parents, carers and other agencies is essential in promoting young people's welfare and in helping young people to be responsible in their approach to online safety

- all children, regardless of age, disability, gender reassignment, race, religion or belief, sex or sexual orientation, have the right to equal protection from all types of harm or abuse.

We will seek to keep children and young people safe by:

- Providing clear and specific directions to staff and volunteers on how to behave online through our behaviour code for adults.
- Supporting and encouraging the young people using our service to use the internet, social media and mobile phones in a way that keeps them safe and shows respect for others.
- Supporting and encouraging parents and carers to do what they can to keep their children safe online
- Developing an online safety agreement for use with young people and their parents or carers.
- Developing clear and robust procedures to enable us to respond appropriately to any incidents of inappropriate online behaviour, whether by an adult or a child or young person.
- Reviewing and updating the security of our information systems regularly.
- Ensuring that user names, logins, email accounts and passwords are used effectively.
- Ensuring personal information about the adults and children who are involved in our organisation is held securely and shared only as appropriate
- Ensuring that images of children, young people and families are used only after permission has been obtained, and only for the purpose for which consent has been given.
- Providing supervision, support and training for staff and volunteers about online safety.
- Examining and risk assessing any social media platforms and new technologies before they are used within the organisation.

If online abuse occurs, we will respond to it by:

- Having clear and robust safeguarding procedures in place for responding to abuse (including online abuse).
- Providing support and training for all staff and volunteers on dealing with all forms of abuse, including bullying or cyberbullying, emotional abuse, sexting, sexual abuse and sexual exploitation.
- Making sure our response takes the needs of the person experiencing abuse, any bystanders and our organisation as a whole into account.
- Reviewing the plan developed to address online abuse at regular intervals, in order to ensure that any problems have been resolved in the long term.

4 areas:

1. **Content** is anything posted online - it might be words or it could be images and video. Children and young people may see illegal, inappropriate or harmful content when online. This includes things like pornography, fake news, racism, misogyny, self-harm, suicide, anti-Semitism, radicalisation and extremism.
2. **Contact** is about the risk of harm young people may face when interacting with other users online. This includes things like peer-to-peer pressure or seeing inappropriate commercial advertising. Sometimes adults pose as children or young adults with the intention of grooming or exploiting a child or young person for sexual, criminal, financial or other purposes.
3. **Conduct** means the way people behave online. Some online behaviour can increase the likelihood, or even cause, harm - for example, online bullying. Conduct also includes things like sharing or receiving nudes and semi-nude images and viewing or sending pornography.

4. **Commerce** is about the risk from things like online gambling, inappropriate advertising, phishing or financial scams. Children and young people may be exposed to these risks directly.

Online safety covers issues relating to children and young people as well as adults and their safe use of the internet, mobile phones and other electronic communications technologies, both in and out of school. It includes education for all members of the school community on risks and responsibilities and is part of the 'duty of care' which applies to everyone working with children.

All members of staff need to be aware of the importance of good online safety practice in the classroom in order to educate and protect the children in their care. Members of staff also need to be informed about how to manage their own professional reputation online and demonstrate appropriate online behaviours compatible with their role.

Breaches of an online safety policy can, and have, led to civil, disciplinary and criminal action being taken against staff, pupils and members of the wider school community.

Current Procedures – In School / Through Portal

Procedure	Details	By Who
Connectivity and Filtering	Internet access is filtered for all users. Differentiated internet access is available for staff and age appropriate access for students / pupils. Customised filtering changes are managed by the school. Illegal content is filtered by broadband or filtering provider by actively employing the Internet Watch Foundation CAIC list and other illegal content lists. Content lists are regularly updated and internet use is logged and frequently monitored. Where personal mobile devices are allowed internet access through the school network, filtering will be applied that is consistent with school practice. Pro-active monitoring alerts the school to breaches of the filtering or Acceptable Use policy, allowing rapid response. There is a clear route for reporting and managing changes to the filtering system. The school monitors content on its network to complement the filtering. There is an appropriate and balanced approach to providing access to online content. The school has adopted Smoothwall Monitor to support in the monitoring and filtering process.	IT Manager
Passwords	All staff must have a password which meets the criteria set in the 360 Safe online safety mark. These requirements are listed below; Not contain the user's account name or parts of the user's full name that exceed two consecutive characters Be at least eight characters in length *Contain characters from three of the following four categories;* English uppercase characters (A through Z) English lowercase characters (a through z) Base 10 digits (0 through 9) Non-alphabetic characters (for example, !, $, #, %)	IT Manager
Technical Security	The school meets the online safety technical requirements outlined in local or national guidelines. There are regular reviews and audits of the safety and security of school computer systems, with oversight from senior leaders and these have impact on policy and practice. The school's computer infrastructure is secure and is not open to misuse or malicious attack.	IT Manager

Online safety Education	There is a planned programme of online safety for all staff and pupils.	PSHE Coordinator

Teaching and Learning

Why is Internet use so important?

The rapid developments in electronic communications are having many effects on society.

- Internet use is part of the statutory curriculum and is a necessary tool for learning.
- The internet is a part of everyday life for education, business and social interaction.
- Cardinal Newman School provides students with quality Internet access as part of their learning experience.
- Pupils use the Internet widely outside school and need to learn how to evaluate Internet information and to take care of their own safety and security.
- The purpose of Internet use in school is to raise educational standards, to promote pupil achievement, to support the professional work of staff and to enhance the school's management functions
- Internet access is an entitlement for students who show a responsible and mature approach to its use.

How does Internet use benefit education?

A number of studies and government projects have identified the educational benefits to be gained through the appropriate use of the Internet including increased pupil attainment.

Benefits of using the Internet in education include:

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

How can internet use enhance learning?

Increased computer numbers and improved Internet access may be provided but its impact on pupils learning outcomes should also be considered. Developing effective practice in using the Internet for teaching and learning is essential. Pupils need to learn digital literacy skills and to refine their own publishing and communications with others via the Internet. Respect for copyright and intellectual property rights, and the correct use of published material should be taught.

- The school's Internet access is designed to enhance and extend education.
- Pupils are taught what Internet use is acceptable and what is not and given clear objectives for internet use.
- The schools will ensure that the copying and subsequent use of Internet-derived materials by staff and pupils complies with copyright law.

- Access levels to the Internet will be reviewed to reflect the curriculum requirements and the age and ability of pupils.
- Staff should guide pupils to online activities that will support the learning outcomes planned for the pupils' age and ability.
- Pupils will be educated in the effective use of the Internet in research, including the shills of knowledge location, retrieval and evaluation.
- Pupils will be taught to acknowledge the source of information used and to respect copyright when using Internet material in their own work.

How will pupils learn how to evaluate content?

The quality of information received via radio, newspaper and telephone is variable and everyone needs to develop critical skills in selection and evaluation. Information received via the Internet, email or text message requires even better information handling and data literacy skills. In particular it may be difficult to determine origin, intent and accuracy, as the contextual clues may be missing or difficult to read. A whole curriculum approach may be required.

- Pupils are taught to be critically aware of the materials they read and are shown how to validate information before accepting its accuracy.
- Pupils will use age-appropriate tools to research Internet content.
- The evaluation of online materials is a part of teaching and learning in every subject and is viewed as a whole-school requirement across the curriculum.

How may email be managed?

Email is an essential means of communication for both staff and pupils. Directed email use can bring significant educational benefits.

All staff understand that they should be using a work provided email account to communicate with parents/carers, pupils and other professionals for official school business only. This is important for confidentiality and security and also to safeguard members of staff from allegations.

The use of email identities such as john.smith@cardinalnewman generally needs to be avoided for younger pupils, as revealing this information could potentially expose a child to identification by unsuitable people. Pupils email accounts will be approved and managed by the school.

- Pupils may only use approved email accounts for school purposes.
- Pupils must immediately tell a designated member of staff if they receive offensive email.
- Pupils must not reveal personal details of themselves or others in email communication, or arrange to meet anyone without specific permission from an adult.
- Staff will only use official school provided email accounts to communicate with pupils and parents/carers, as approved by the Senior Leadership Team.
- Access in school to external personal email accounts may be blocked.
- Excessive social email use can interfere with learning and will be restricted.
- Email sent to external organisations should be written carefully and authorised before sending, in the same way as a letter written on school headed paper would be.
- The forwarding of chain messages is not permitted.
- Staff should not use personal email accounts during school hours or for professional purposes.

- The contact details on the website should be the school address, email and telephone number. Staff or pupils' personal information must not be published.
- The Head teacher will take overall editorial responsibility for online content published by the school and will ensure that content published is accurate and appropriate.
- The school website will comply with the schools' guidelines for publications including respect for intellectual property rights, privacy policies and copyright.

Can pupils' images or work be published?

Still and moving images and sound add liveliness and interest to a publication, particularly when pupils can be included. Nevertheless, the security of staff and pupils is paramount. Although common in newspapers, the publishing of pupils' names with their images is not acceptable. Published images could be reused, particularly if large images of individual pupils are shown. Images of a pupil should not be published without the parent's or carer's written permission.

- Images or videos that include pupils will be selected carefully and will not provide material that could be reused.
- Pupil's full names will not be used anywhere on the website, particularly in association with photographs.
- Written permission from parents or carers will be obtained before images/videos of pupils are electronically published.
- Pupils work can only be published with their permission or the parents.
- Written consent will be kept by the school where pupil's images are used for publicity purposes, until the image is no longer in use.

How will social networking, social media and personal publishing be managed?

Parents, Staff and Students need to be aware that the internet has emerging online spaces and social networks which allow individuals to publish unmediated content. Social networking sites can connect people with similar or even very different interests. Users can be invited to view personal spaces and leave comments, over which there may be limited control. For responsible adults, social networking sites provide easy to use, free facilities, although advertising often intrudes and some sites may be dubious in content. Pupils are encouraged to think about the ease of uploading personal information, the associated dangers and the difficulty of removing an appropriate image or information once published.

All staff are aware of the potential risks of using social networking sites or personal publishing either professionally with students or personally. They are aware of the importance of considering the material they post, ensuring profiles are secured and how publishing unsuitable material may affect their professional status.

- The school controls access to social media and social networking sites.
- Parents, Staff and Students are advised never to give out personal details of any kind which may identify them and /or their location. Examples would include real name, address, mobile or landline phone numbers, school attended, IM and email addresses, full names of friends/family, specific interests and clubs etc.
- Staff wishing to use Social Media tools with students must ensure the site is age appropriate.
- Staff official blogs must be monitored and approved by The Headteacher and/or School Network Manager. Members of staff are advised not to run social networking spaces for pupil use on a personal basis.

How should personal data be protected?

The Data Protection Act 2018 controls how your personal information is used by organisations, businesses or the government. The Data Protection Act 2018 is the UK's implementation of the General Data Protection Regulation (GDPR).

Everyone responsible for using personal data has to follow strict rules called 'data protection principles'. They must make sure the information is:

- used fairly, lawfully and transparently
- used for specified, explicit purposes
- used in a way that is adequate, relevant and limited to only what is necessary
- accurate and, where necessary, kept up to date
- kept for no longer than is necessary
- handled in a way that ensures appropriate security, including protection against unlawful or unauthorised processing, access, loss, destruction or damage

There is stronger legal protection for more sensitive information, such as:

- race
- ethnic background
- political opinions
- religious beliefs
- trade union membership
- genetics
- biometrics (where used for identification)
- health
- sex or orientation

There are separate safeguards for personal data relating to criminal convictions and offences.

Your rights

Under the Data Protection Act 2018, you have the right to find out what information the government and other organisations store about you. These include the right to:

- be informed about how your data is being used
- access personal data
- have incorrect data updated
- have data erased
- stop or restrict the processing of your data
- data portability (allowing you to get and reuse your data for different services)
- object to how your data is processed in certain circumstances

You also have rights when an organisation is using your personal data for:

- automated decision-making processes (without human involvement)
- profiling, for example to predict your behaviour or interests

Policy Decisions

How will internet access be authorised?

The school will allocate Internet access to staff and pupils on the basis of educational need. Parental permission must be given for internet access in all cases. Students will not be prevented from accessing the internet unless their parents have specifically denied permission.

The school maintains a current record of all staff and pupils who are granted access to the school's electronic communications.
All staff read the School Acceptable use policy before using any school ICT resources. Parents are asked to read the School Acceptable Use Policy for students' access and discuss it with their child, where appropriate. All visitors to the school site who require access to the school's network or internet access are asked to read and sign an Acceptable Use Policy.
Parents are informed that pupils will be provided with supervised Internet access appropriate to their age and ability.

How will risks be assessed?

- The school takes all reasonable precautions to ensure that users access only appropriate material. However, due to the global and connected nature of the Internet content, it is not possible to guarantee that access to unsuitable material will never occur via a school computer.
- The school audit's ICT use to establish if the online safety policy is adequate and that the implementation of the online safety policy is appropriate.
- The use of computer systems without permission or for inappropriate purposes could constitute a criminal offence under the Computer Misuse Act 1990 and breeches will be reported to the Police.
- Methods to identify, assess and minimise risks are reviewed regularly.

How will the school respond to any incidents of concern?

Internet technologies and electronic communications provide children with exciting opportunities to broaden their learning experiences and develop creativity in and out of school. However, there are risks associated with the way these technologies can be used. The school recognises and seeks to develop the skills that children and young people need when communicating and using technologies enabling them to keep safe and secure and act with respect for others. Online safety risks can be experienced unintentionally or deliberately by people acting inappropriately or even illegally. Any potential concerns are dealt with by the designated officer. Teachers are the first line of defence; their observation of behaviour is essential in recognising concerns about pupils and in developing trust so that issues are reported.

Staff also help to develop a safe culture by observing each other's behaviour online and discussing together any potential concerns. Incidents of concern may include unconsidered jokes and comments or inappropriate actions. Any illegal or Prevent related activity or should be reported to the school Designated Child Protection Coordinator.

- All members of the school community are informed about the procedure for reporting online safety concerns (such as breaches of filtering, cyberbullying, accessing extremist or terrorist related material for non-educational purposes, illegal content etc).

- The Designated Child Protection Coordinator is informed of any online safety incidents involving Child Protection, Prevent or any Safeguarding concerns, which will then be escalated appropriately.
- The school will inform parents/carers of any incidents of concerns as and when required.
- Where there is cause for concern or fear that illegal activity has taken place or is taking place then the school will contact the Children's Safeguarding Team and escalate the concern to the Police.

How will Cyberbullying be managed?

Cyberbullying can be defined as "The use of Information Communication Technology, particularly mobile phones and the internet to deliberately hurt or upset someone" DCSF 2007.

Many young people and adults find that using the internet and mobile phones is a positive and creative part of their everyday life. Unfortunately, technologies can also be used negatively. When children are the target of bullying via mobile phones, gaming or the Internet, they can often feel very alone, particularly if the adults around them do not understand cyberbullying and its effects. A once previously safe and enjoyable environment or activity can become threatening, harmful and a source of anxiety. It is essential that children, school staff and parents and carers understand how cyberbullying is different from other forms of bullying, how it can affect people and how to respond and combat misuse. Promoting a culture of confident users will support innovation and safety.

Where bullying outside school (such as online or via text) is reported to the school, it will be investigated and acted on.

It is important to bear in mind that some types of harassing or threatening behaviour or communications could be a criminal offence, for example under the Protection from Harassment Act 1997, the Malicious Communications Act 1998, the Communications Act 2003, and the Public Order Act 1986. If a member of staff feels that an offence may have been committed towards them they should seek assistance from the School and Police.

- Cyberbullying (along with all other forms of bullying) of any member of the school community will not be tolerated.
- There are clear procedures in place to support anyone in the school community affected by cyberbullying.
- All incidents of cyberbullying reported to the school are recorded.
- There are clear procedures in place to investigate incidents or allegations of Cyberbullying.
- Pupils, staff and parents/carers are advised to keep a record of the bullying as evidence.
- The school will take steps to identify the bully, where possible and appropriate. This may include examining school system logs, identifying and interviewing possible witnesses, and contacting the service provider and the police, if necessary.
- Pupils, staff and parents/carers are required to work with the school to support the approach to cyberbullying and the school's online safety ethos.

Sanctions for those involved in cyberbullying may include:

1. The bully will be asked to remove any material deemed to be inappropriate or offensive.
2. A service provider may be contacted to remove content if the bully refuses or is unable to delete content.
3. Internet access may be suspended at school for the user for a period of time.
4. Parent/carers of pupils will be informed.
5. The Police will be contacted if a criminal offence is suspected.

How will learning platforms be managed?

An effective learning platform (LP) or learning environment can offer school a wide range of benefit to teachers, pupils and parents, as well as support for management and administration. It can enable pupils and teachers to collaborate in and across schools, sharing resources and tools for a range of topics. It also enables the creation and management of digital content and pupils can develop online and secure e-portfolios to showcase examples of work.

- SLT and staff will regularly monitor the usage of the LP by pupils and staff in all areas, in particular message and communication tools and publishing facilities.
- Pupils/staff are advised about acceptable conduct and use when using the LP.
- Only members of the current pupil, parent/carers and staff community will have access to the LP.
- All users will be mindful of copyright issues and should only upload appropriate content onto the LP.
- When staff, pupils etc, leave the school their account or rights to specific school areas are disabled or transferred to their new establishment.

- Any concerns about content on the LP will be recorded and dealt with in the following ways:

1. The user will be asked to remove any material deemed to be inappropriate or offensive.
2. The material will be removed by the site administrator if the user does not comply.
3. Access to the LP for the user may be suspended.
4. The user will need to discuss the issues with a member of SLT before reinstatement.
5. A pupils' parent/carer will be informed.

- A visitor may be invited onto the LP by a member of the SLT. In this instance there may be an agreed focus or a limited time slot.
- Pupils may require editorial approval from a member of staff. This may be given to the pupil to fulfil a specific aim and may have a limited time frame.

How will mobile phones and personal devices be managed?

Mobile phones and other personal devices such as Games Consoles, Tablets, PDA, MP3 Players etc. are considered to be an everyday item in today's society and even children in early years settings may own and use personal devices to get online regularly. Mobile phones and other internet enabled personal devices can be used to communicate in a variety of ways with texting, camera phones and internet accesses all common features.

However, mobile phones can present a number of problems when not used appropriately:

- They are valuable items which may be stolen or damaged;
- Their use can render pupils or staff subject to cyberbullying;
- Internet access on phones and personal devices can allow pupils to bypass school security settings and filtering.
- They can undermine classroom discipline as they can be used on "silent" mode;
- Mobile phones with integrated cameras could lead to inappropriate capture, use or distribution of images of pupils or staff.
- The sending of abusive or inappropriate messages or content via mobile phones or personal devices is forbidden by any member of the school community and any breaches will be dealt with.
- School staff may confiscate a phone or device if they believe it is being used to contravene the school behaviour policy. The phone or device might be searched by the Senior Leadership Team with the consent of the pupil or parent/carer. If there is suspicion that the material on the mobile may provide evidence relating to a criminal offence the phone will be handed over to the police for further investigation.

- Mobile phones will not be used during lessons or formal school time unless as part of an approved and directed curriculum-based activity with consent from a member of staff.
- Electronic devises of all kinds that are brought into school are the responsibility of the user. The school accepts no responsibility for the loss, theft or damage of such items. Nor will the school accept responsibility for any adverse health effects caused by any such devices either potential or actual.
- Mobile phones and personal devices are not permitted to be used in certain areas within the school site such as changing rooms, toilets and swimming pools.

Pupils use of personal devices.

- If a pupil breaches the school policy then the phone or device will be confiscated and will be held in a secure place in the school office.
- Phones and devices, including smart watches must not be taken into examinations. Pupils found in possession of a mobile phone or smart watch during an exam will be reported to the appropriate examining body. This may result in the student's withdrawal from either that examination or all examinations.
- Parents are advised not to contact their child via mobile phone during the school day, but to contact the school office.
- Students are regularly reminded that they should protect their phone numbers by only giving them to trusted friends and family members. Students are instructed in safe and appropriate use of mobile phones and personal devices and are made aware of boundaries and consequences.

Staff Use of Personal Devices

- Staff are not permitted to use their own personal phones or devices for contacting children, young people and their families within or outside of the setting in a professional capacity.
- If members of staff have an educational reason to allow children to use mobile phones or personal devices as part of an educational activity then it will only take place when approved by the Senior Leadership Team.
- Staff must not use personal devices such as mobile phones or cameras to take photos or videos of pupils and should only use work-provided equipment for purpose.
- If a member of staff breaches the school policy then disciplinary action may be taken.

The Governing Body approved this policy on date:

Signed: Chair of Governors

Signed: Headteacher