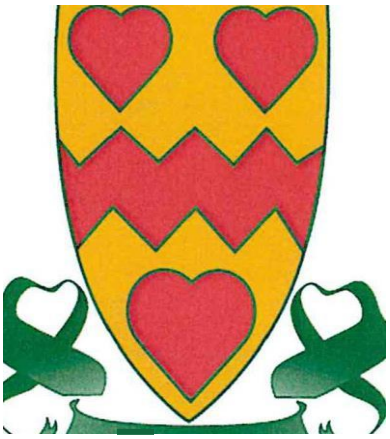
I



E-SAFETY POLICY

GOVERNING BODY APPROVAL:

AUTUMN TERM – **OCTOBER 2020/21**

COMMITTEE WITH RESPONSIBILITY FOR MONITORING AND REVIEW:

PERSONNEL COMMITTEE

NEXT REVIEW DATE: **AUTUMN 2021/22**

Newman Catholic College

E-Safety Policy

lntroduction

This policy refers to and encompasses the use of computers, internet technologies and other forms of electronic communications by students and staff at Newman Catholic College. It highlights the need to educate children and young people about the benefits and risks of using new technologies and details the safeguards that are in place to enable them to use ICT safely. The requirement to ensure that children and young people are able to use the internet and related communications technologies appropriately and safely is addressed as part of the wider duty of care to which all who work in schools are bound. A school E-Safety policy should help to ensure safe and appropriate use. Newman Catholic College must demonstrate that it has provided the necessary safeguards to help ensure it has done everything that could reasonably be expected of it to manage and reduce these risks.

Links to other policies

This policy makes reference to the new Acceptable Use Policy statement for both staff and pupils. A copy of this statement can be found in Appendix 1. It applies to all members of the school community (including staff, pupils, volunteers, parents / carers, visitors, community users) who have access to and are users of school ICT systems, both in and out of school.

The E-Safety policy should be reviewed in line with the following policies:

- Child Protection
- Anti-Bullying
- Behaviour
- Data Protection

Newman Catholic College recognises that ICT and the internet are fantastic tools for learning and communication that can be used in school to enhance the curriculum, challenge students, and support creativity and independence. Using ICT to interact socially and share ideas can benefit everyone in the school community, but it is important that the use of the internet and ICT is seen as a responsibility and that students, staff and parents use it appropriately and practice good e-safety. It is important that all members of the school community are aware of the dangers of using the internet and how they should conduct themselves online.

E-safety covers the internet but it also covers mobile phones and other electronic communications technologies. We know that some adults and young people will use these technologies to harm children. The harm might range from sending hurtful or abusive texts and emails, to enticing children to engage in sexually harmful conversations or actions online, webcam filming, photography or face-to-face meetings. There is a 'duty of care' for any persons working with children and educating all members of the school community on the risks and responsibilities of e• safety. It is important that there is a balance between controlling access to the internet and technology and allowing freedom to explore and use these tools to their full potential. This policy aims to be an aid in regulating ICT activity in school, and provide a good understanding of appropriate ICT use that members of the school community can use as a reference for their conduct online outside of school hours. E-safety is a whole-school issue and responsibility.

Cyber-bullying by students will be treated as seriously as any other type of bullying and will be managed through our behaviour and anti-bullying procedures which are outlined in our Behaviour for Progress and Anti-Bullying policies.

I • Roles and Responsibility

The following section outlines the e-safety roles and responsibilities of individuals and groups within the school.

The School E-Safety Coordinators are:

Technical Ms S Grace Assistant Headteacher
Safeguarding Mr A Dunne Deputy Headteacher
Governing Body responsible for E-Safety is:

Governors

C

Governors are responsible for the approval of the E-Safety Policy and for reviewing the effectiveness of the policy. This will be carried out by the Governors receiving regular information about e-safety incidents and monitoring reports. A member of the Governing body has taken on the role of E-Safety Governor. The role of the E-Safety Governor will include:

regular meetings with the E-Safety Co-ordinators
regular monitoring of e-safety incident logs
regular monitoring of filtering / change control logs
reporting to Governors meetings

Headteacher and Senior Leaders

The Headteacher has a duty of care for ensuring the safety (including e• safety) of members of the school community, though the day to day responsibility for e-safety will be delegated to the E-Safety Co-ordinators.

The Headteacher and Senior Leaders are aware of the procedures to be followed in the event of a serious e-safety allegation being made against a member of staff

C

The Headteacher and the Designated Safeguarding Lead are responsible for ensuring that the E-Safety Co-ordinators and all other members of staff receive suitable training to enable them to carry out their e-safety roles.

The Senior Leadership Team will receive regular monitoring reports from the E-Safety Co-ordinators.

E-Safety Co-ordinators takes day to day responsibility for e-safety issues and has a leading role in establishing and reviewing the school e-safety policies and documents

E-Safety Co-ordinator ensures that all staff are aware of the procedures that need to be followed in the event of an e-safety incident taking place

E-Safety Co-ordinators provide training and advice for staff

E-Safety Co-ordinators liaise with the Local Authority

E-Safety Co-ordinators liaise with school technical staff

E-Safety Co-ordinators receive reports of e-safety incidents and creates a log of incidents to inform future e-safety developments

E-Safety Co-ordinators meets regularly with the E-Safety Governor to discuss current issues, review incident logs and filtering/ change control logs

E-Safety Co-ordinators report regularly to the Senior Leadership team

Network Manaqer / Technical Staff

The Network Manager is responsible for ensuring:

- that the school's technical infrastructure is secure and is not open to misuse or malicious attack
- that the school meets required safety technical requirements and any Local Authority E-Safety Guidance that may apply
- that users may only access the networks and devices through a properly enforced password protection policy, in which passwords are regularly changed
- that the filtering policy is applied
- that they keep up to date with e-safety technical information in order to effectively carry out their e-safety role and to inform and update others as relevant
- that the use of the network / internet / Virtual Learning Environment/ remote access / e-mail is regularly monitored in order that any misuse or attempted misuse can be reported to the Headteacher and E-Safety Co-ordinators
- that monitoring software / systems are implemented and updated as agreed with the Headteacher

C

<u>Teaching and Support Staff</u>

Teaching and support staff are responsible for ensuring that:

- they have an up to date awareness of e-safety matters and the current school e-safety policy and practices
- they have read, understood and signed the Staff Acceptable Use Agreement
- that they report any suspected misuse or problem to the Headteacher and E• Safety Co-ordinators for investigation / action / sanction
- all digital communications with students / parents / carers should be on a professional level and only carried out using school systems
- e-safety issues are embedded in all aspects of the curriculum and other activities
- students understand and follow the e-safety and Acceptable Use Agreements
- students have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations
- they monitor the use of digital technologies, mobile devices, cameras etc. in lessons and other school activities and implement current policies with regard to these devices
- in lessons where internet use is pre-planned students are guided to sites that have been checked as suitable and that processes are in place for dealing with any unsuitable material that is found in internet searches

C

<u>Designated Safeguarding Leads</u>

Should be trained in e-safety issues and be aware of the potential serious safeguarding / child protection issues to arise from:

- sharing of personal data
- access to illegal / inappropriate materials
- inappropriate on-line contact with adults/ strangers
- potential or actual incidents of grooming
- cyber-bullying

It is important to emphasise that these are child protection issues, not technical issues simply that the technology provides additional means for child protection issues to develoo.

Students

- are responsible for using the school digital technology systems in accordance with the Student Acceptable Use Agreement
- have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations
- need to understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so
- will be expected to know and understand policies on the use of mobile devices and digital cameras
- will be expected to know and understand policies on the taking/ use of images and on cyber-bullying
- should understand the importance of adopting good e-safety practice when using digital technologies out of school and realise that the school's E-Safety Policy covers their actions out of school, if related to their membership of the school

Parents/Carers

Parents/Carers play a crucial role in ensuring that their children understand the need to use the internet / mobile devices in an appropriate way. The school will take very opportunity to help parents/carers understand these issues through parents' evenings, letters, website, VLE and information about national / local e-safety campaigns and literature. Parents and carers will be encouraged to support the school in promoting good e-safety practice and to follow guidelines on the appropriate use of:

digital and video images taken at school

access to parents' sections of the website / VLE and online student records

their children's personal devices in the school

2. Communicatin1 School Policy

This policy is available from the school office and on the school website for parents/carers, staff, and students to access when and as they wish. Rules relating to the school code of conduct when online, and e-safety guidelines, are displayed around the school. E-safety is integrated into the curriculum in any circumstance where the internet or technology are being used, and during lessons where personal safety, responsibility, and/or development are being discussed.

Parents and carers play an essential role in the education of their children and in the monitoring / regulation of the children's on-line behaviours. We will therefore seek to provide information and awareness to parents and carers through curriculum activities, the website and high profile events and campaigns e.g. Safer Internet Day.

;1. Trainin1

Staff

It is essential that all staff receive e-safety training and understand their responsibilities, as outlined in this policy. Training will be offered as follows:

annual on-line e-safety training

all new staff will receive e-safety training as part of their induction programme, ensuring that they fully understand the school e-safety policy and Acceptable

Use Agreements

the E-Safety Co-ordinators will receive regular updates through attendance at external training events and by reviewing guidance documents released by relevant organisations

this E-Safety Policy and its updates will be presented to and discussed by staff on inset days and in meetings

the E-Safety Co-ordinators will provide advice /guidance/ training to individuals as required

Governors

Governors will be invited to take part in e-safety training / awareness sessions with particular importance for those who are members of any committee involved in technology, e-safety, health and safety and safeguarding / child protection. This may be offered in a number of ways:

attendance at training provided by the Local Authority / National Governors Association/ or other relevant organisations

participation in school training / information session for staff or parents

4, Nakjn9 use of ICT and 1he ln1erne1 jn School

The internet is used in school to raise educational standards, to promote student achievement, to support the professional work of staff and to enhance the school's management functions. Technology is advancing rapidly and is now a huge part of everyday life, education and business. We want to equip our students with all the necessary ICT skills that they will need in order to enable them to progress confidently into a professional working environment when they leave school.

Some of the benefits of using ICT and the internet in schools are:

For students:

Unlimited access to worldwide educational resources and institutions such as art galleries, museums and libraries.

Contact with schools in other countries resulting in cultural exchanges between students all over the world.

Access to subject experts, role models, inspirational people and organisations. The internet can provide a great opportunity for students to interact with people that they otherwise would never be able to meet.

An enhanced curriculum; interactive learning tools; collaboration, locally, nationally, and globally; self-evaluation; feedback and assessment; updates on current affairs as they happen.

Access to learning whenever and wherever convenient.

Freedom to be creative.

Freedom to explore the world and its cultures from within a classroom.

Social inclusion, in class and online.

Access to case studies, videos and interactive media to enhance understanding.

Individualised access to learning

Staff

Professional development through access to national developments, educational materials and examples of effective curriculum practice and classroom strategies.

Immediate professional and personal support through networks and associations.

Improved access to technical support.
Ability to provide immediate feedback to students and parents.
Class management, attendance records, schedule, and assignment tracking.

Parents

The majority of communication between the school and parents/carers is via e-mail. This form of contact is considered to be more effective, reliable and economic.
Text messages and letters will also inform parent/carers of details relating to attendance and behaviour.

5, Learnina to evaluate Internet Content

With so much information available online it is important that students learn how to evaluate internet content for accuracy and intent. This is approached by the school as part of digital literacy across all subjects in the curriculum. Students will be taught:

- to be critically aware of materials they read, and shown how to validate information before accepting it as accurate
- to use age-appropriate tools to search for information online
- to acknowledge the source of information used and to respect copyright.

Plagiarism is against the law and the school will take any intentional acts of plagiary very seriously. Students who are found to have plagiarised will be disciplined. If they have plagiarised in an exam or a piece of coursework, they may be prohibited from completing that exam.

The school will also take steps to filter internet content to ensure that it is appropriate to the age and maturity of students. If staff or students discover unsuitable sites then the URL will be reported to the school E• Safety Co-ordinator. Any material found by members of the school community that is believed to be unlawful will be reported to the appropriate agencies. Regular software and broadband checks will take place to ensure that filtering services are working effectively.

I, Mana9in9 Information Systems

The school is responsible for reviewing and managing the security of the computers and internet networks as a whole and takes the protection of school data and personal protection of our school community very. seriously. This means protecting the school network, as far as is practicably possible, against viruses, hackers and other external security threats. The security of the school information systems and users will be reviewed regularly by the Network Manager and virus protection software will be updated regularly. Some safeguards that the school takes to secure our computer systems are:

- ensuring that all personal data sent over the internet or taken off site is encrypted
- making sure that unapproved software is not downloaded to any school computers. Alerts will be set up to warn users of this
- files held on the school network will be regularly checked for viruses
- the use of user logins and passwords to access the school network will be enforced
- portable media containing school data or prograrr1rT1es will not beJaken off-

site without specific permission from a member of the senior leadership team.
termly reporting to Governors

For more information on data protection in school please refer to our data protection policy.

1. School Email Accounts and Appropriate Use

The school uses email internally for staff and students and externally for contacting parents, and is an essential part of school communication.
Staff and students should be aware that school email accounts should only be used for school related matters, ie. For staff to contact parents, other members of staff and other professionals for work purposes. This is important for confidentiality. The school has the right to monitor emails and their contents but will only do so if it feels there is a reason to.
Staff should be aware of the following when using email in school:

- Staff should only use official school-provided email accounts to communicate with students, parents and carers. Personal email accounts should not be used to contact any of these people for school business.
- Emails sent from school accounts should be professionally and carefully written. Staff are representing the school at all times and should take this into account when entering into any email communications
- Staff must tell their manager of a member of the senior leadership team if they receive any offensive threatening or unsuitable emails either from within the school or from and external account. They should not attempt to deal with this themselves.
- The forwarding of chain message is not permitted in school
- Students will be educated through the ICVT curriculum to identify spam, phishing and virus emails and attachments that could cause harm to the school network or their personal account or well being

a. Published Content and the School Website

The school website is viewed as a useful tool for communicating our school ethos and practice to the wider community. It is also a valuable resource for parents/carers, students, and staff for keeping up-to-date with school news and events, celebrating whole-school achievements and personal· achievements, and promoting school projects.

The website is in the public domain, and can be viewed by anybody online. Any information published on the website will be carefully considered in terms of safety for the school community, copyrights and privacy policies. No personal information on staff or students will be published, and details for contacting the school will be for the school office only.

Policy and guidance of safe use of student's photographs and work
Colour photographs and students work bring our school to life, showcase our student's talents, and add interest to publications both online and in print that represent the school. However, the school acknowledges the importance of having safety precautions in place to prevent the misuse of such material.
Newman Catholic College believes that celebrating the achievement of children in school is an important part of their learning experience and personal development.

Taking photographs and videos of students for internal display and displaying student work for educational use enables us to celebrate individual and group successes as a school community.
However, we would also like to use photographs and videos of the school and its students externally for promotional purposes (in the public domain) and in order to promote the good educational practice of the school but in accordance with the Data Protection Act 1998 we will only do this with parent/carer consent. On admission to the school parents/carers will be asked to sign an Acceptable Use Agreement which incorporates digital/video permissions.
By signing this form parents/carers will be consenting to the use of images of their son/daughter being used in the following outlets:
• all schoolpublications
• on the school website
• in newspapers as allowed by the school
• in videos made by the school or in class for school projects
The form covers consent for the duration of their son/daughter's time at the school. Student's full names will never be published externally with their photographs, but may be published internally (for example, on display with their work).

C1

Using photographs of individual children
The vast majority of people who take or view photographs or videos of children do so for entirely innocent, understandable and acceptable reasons. Sadly, some people abuse children through taking or using images, so we must ensure that we have some safeguards in place.
It is important that published images do not identify students or put them at risk of being identified. Only images created by or for the school will be used in public and children may not be approached or photographed while in school or doing school activities without the school's permission. The school follows general rules on the use of photographs of individual children:

- Parental consent must be obtained for external/promotional use.
- Electronic and paper images will be stored securely.
- Images will be carefully chosen to ensure that they do not pose a risk of misuse. This includes ensuring that students are appropriately dressed.
- Photographs of activities which may pose a greater risk of potential misuse (for example, swimming activities), will focus more on the sport than the students (i.e. a student in a swimming pool, rather than standing by the side in a swimsuit).
- For public documents, including in newspapers, full names will not be published alongside images of the child. Groups may be referred to collectively by year group or form name.
- Events recorded by family members of the students such as school plays or sports days must be used for personal use only.
- Students are encouraged to tell a member staff if they are concerned or uncomfortable with any photographs that are taken of them or they are being asked to participate in.
- Any photographers that are commissioned by the school will be fully briefed on appropriateness in terms of content and behaviour, will wear identification at all times, and will not have unsupervised access to the students. For more information on safeguarding in school please refer to our school safeguarding and child protection policy.

0

Complaints of misuse of photographs or video- Parents should follow standard school complaints procedure if they have a concern or complaint regarding the misuse of school photographs

••Social neiworkina, social media and personal publishina

Personal publishing tools include biogs, wikis, social networking sites, bulletin boards, chat rooms and instant messaging programmes. These online forums are the more obvious sources of inappropriate and harmful behaviour and where students are most vulnerable to being contacted by a dangerous person. It is important that we educate students so that they can make their own informed decisions and take responsibility for their conduct online.

Social media sites have many benefits for both personal use and professional learning; however, both staff and students should be aware of how they present themselves online.

("1

Students are taught through the ICT curriculum about the risks and responsibility of uploading personal information and the difficulty of taking it down completely once it is out in such a public place.

The school follows general rules on the use of social media and social networking sites in school:

- Students are educated on the dangers of social networking sites such as Facebook, lnstragram, Snapchat, What's App,Twitter etc and how to use them in safe and productive ways. They are all made fully aware of the school's code of conduct regarding the use of ICT and technologies and behaviour online.
- Any sites that are to be used in class will be risk-assessed by the teacher in charge prior to the lesson to ensure that the site is age-appropriate and safe for use.
- Official school biogs created by staff or students/year groups/school clubs as part of the school curriculum will be password-protected and run with the approval of a member of staff and will be moderated by a member of staff.
- Students and staff are encouraged not to publish specific and detailed private thoughts, especially those that might be considered hurtful, harmful or defamatory. The school expects all staff and students to remember that they are representing the school at all times and must act appropriately.
- Safe and professional behaviour of staff online will be discussed at staff induction.

0

I 0.Mobile Phones and Personal Devices

While mobile phones and personal communication devices are common place in today's society, their use and the responsibility for using them should not be taken lightly.

Some issues surrounding the possession of these devices are:

- they can make students and staff more vulnerable to cyberbullying
- they can be used to access inappropriate internet material
- they can be a distraction in the classroom
- they are valuable items that could be stolen, damaged, or lost
- they can have integrated cameras, which can lead to child protection, bullying

and data protection issues.

•!•

The school therefore adopts a zero tolerance Electronic Device Policy for students during the school day:

Phones and electronic devices (including headphones) will be confiscated
The incident will be logged on our behaviour management system.
Any student who refuses to hand over the complete phone (battery and SIM card) / device when requested will be removed from the lesson by either by a member of the senior leadership team. This in turn will lead to a 1 day internal exclusion in the first event and then a fixed term exclusion for repeat offences.
In circumstances where there is a suspicion that material on a phone is unsuitable the phone will be handed over to the Police for further investigation.

We do however; understand that a parent/carer may Wish for their son to have a mobile phone for their journey to and from school. In this situation a student should hand his phone/device into the school office.

Emergencies:

If a student needs to contact his parents/carers they will be allowed to use a school phone.
If parents/carers need to contact their son(s) urgently they should phone the school office and a message will be relayed promptly.

Responsibility:

Newman Catholic College accepts no responsibility whatsoever for theft, loss or damage relating to phones/devices including those handed in/confiscated.
Newman Catholic College will not investigate theft, loss or damage relating to phones/devices.

Staff

• Under no circumstances should staff use their own personal devices to contact students or parents either in or out of school time unless in an emergency.
• Staff are not permitted to take photos or videos of students. If photos or videos are being taken as part of the school curriculum or for a professional capacity, the school equipment will be used for this.
• The school expects staff to lead by example. Personal mobile phones should be switched off or on'silent' during school hours.
• Any breach of school policy may result in disciplinary action against that member of staff.

11. Cyberbullying

Cyberbullying, as with any other form of bullying, is taken very seriously by the school. Information about specific strategies or programmes in place to prevent and tackle bullying are set out in the anti-bullying policy. The anonymity that can come with using the internet can sometimes make people feel safe to say and do hurtful things that they otherwise would not do in person. It is made very clear to members of the school community what is expected of them in terms of respecting their peers, members of the public and staff, and any intentional breach of this will result in disciplinary action.

If an allegation of bullying does come up, the school will:

take it seriously
act as quickly as possible to establish the facts. It may be necessary to examine school systems and logs or contact the service provider in order to

identify the bully
record and report the incident
provide support and reassurance to the victim
make it clear to the 'bully' that this behaviour will not be tolerated.
If there is a group of people involved, they will be spoken to individually and as a whole group. It is important that children who have harmed another, either physically or emotionally, redress their actions and the school will make sure that they understand what they have done and the impact of their actions.

If a sanction is used, it will correlate to the seriousness of the incident and the 'bully' will be told why it is being used. They will be asked to remove any harmful or inappropriate content that has been published, and the service provide may be contacted to do this if they refuse or are unable to remove it. They may have their internet access suspended in school.
Repeated bullying may result in a fixed-term exclusion.

C

Funher E-Safecy Advice

http://www.getsafeonline.org/

http://www.kidscape.org.uk/childrenteens/cyberbullying.shtml

http://www.thinkuknow.co.uk/

http://www.chatdanger.com/
http://www.kidscape.org.uk/childrenteens/cyberbullying.shtml

https://www.ceop.police.uk/

C

Appendix I

Newman
Catholic College
ExcellenceThrough Faith

E- Sa fety

RESPONSIBLE E SAFETY and INTERNET USE POLICY

Rules for Staff and Students

The computer system is owned by the school. This Responsible Internet Use statement helps to protect students, staff and the school by clearly stating what use of the computer resources is acceptable and what is not.

- Irresponsible use may result in the loss of Internet access
- Network access must be made via the user's authorised account and password, which must not be given to any other person
- School computer and Internet use must be appropriate to the student's education or to staff professional activity
- Copyright and intellectual property rights must be respected
- The school lCT systems may not be used for private purposes, unless the headteacher has given permission for that use
- Use for personal financial gain, gambling, political purposes or advertising is not permitted
- ICT system security must be respected; it is a criminal offence to use a computer for a purpose not permitted by the system owner

RESPONSIBLE INTERNET USE

These rules help us to be fair to others and keep everyone safe

- I will ask permission before using the Internet
- I will use only my own network login and password, which is secret
- I will only look at or delete my own files
- I understand that I must not bring software or memory sticks into school without permission
- If I see anything I am unhappy with or I receive messages I do not like, I will tell a teacher immediately
- I understand that the school may check my computer files and the Internet sites I visit
- I understand that if I deliberately break these rules, I may not be allowed to use the Internet or computers.

Signed.....