CARDINAL NEWMAN CATHOLIC SCHOOL

November 2018

Date of Next Review:
November 2019

E-Safety and Use of Social Media Policy

E-SAFETY AND USE OF SOCIAL MEDIA POLICY

Cardinal Newman Catholic School is committed to safeguarding and promoting the welfare of children and young people and expects all staff, volunteers and visitors to the school to share this commitment.

SLT Responsibility: CJ

Safeguarding Governor: Bernadette Hopper

The Policy Document

The Internet and related technologies are powerful tools, which open up new prospects for communication and collaboration. Education is embracing these new technologies as they bring with them fresh opportunities for both teachers and learners.

The 'staying safe' outcome includes aims that children and young people are:

- safe from maltreatment, neglect, violence and sexual exploitation
- safe from accidental injury and death
- safe from bullying and discrimination
- safe from crime and anti-social behaviour in and out of school
- secure, stable and cared for

Much of these aims apply equally to the 'virtual world' that children and young people will encounter whenever they use ICT in its various forms. For example, we know that the internet has been used for grooming children and young people with the ultimate aim of exploiting them sexually; we know that ICT can offer weapons for bullies, who may torment their victims via websites or text messages; and we know that children and young people have been exposed to inappropriate content when online, which can sometimes lead to their involvement in crime and anti-social behaviour.

It is the duty of the school to ensure that every child in their care is safe, and the same principles should apply to the 'virtual' or digital world as would be applied to the school's physical buildings.
This Policy document is drawn up to protect all parties – the students, the staff and the school and aims to provide clear advice and guidance on how to minimise risks and how to deal with any infringements.

1. The technologies

ICT in the 21st Century has an all-encompassing role within the lives of children and adults. New technologies are enhancing communication and the sharing of information. Current and emerging technologies used in school and, more importantly in many cases, used outside of school by children include:

- The Internet
- E-mail
- Instant messenger

- Blogs
- Podcasting (radio / audio broadcasts downloaded to computer or MP3/4 player)
- Social networking sites
- Video broadcasting sites
- Chat Rooms
- Gaming Sites
- Music download sites
- Mobile phones with camera and video functionality
- Smart phones

2. Whole school approach to the safe use of ICT

Creating a safe ICT learning environment includes three main elements at the school:

- An effective range of technological tools
- Policies and procedures, with clear roles and responsibilities
- E-Safety advice and information for staff and parents and an E-Safety Education Programme for students

3. Roles and Responsibilities

E-Safety is recognised as an essential aspect of strategic leadership in this school and the Principal, with the support of Governors, aims to embed safe practices into the culture of the school. The Principal ensures that the policy is implemented and compliance with the policy monitored.

Our school senior designated person for safeguarding is: CJ

All teachers are responsible for promoting and supporting safe behaviours in their classrooms and following school e-Safety procedures. Central to this is fostering a 'No Blame' culture so students feel able to report any bullying, abuse or inappropriate materials.

All staff should be familiar with the schools' Policy including:

- Safe use of e-mail
- Safe use of Internet
- Safe use of school network, equipment and data
- Safe use of digital images and digital technologies, such as mobile phones and digital cameras
- Publication of pupil information/photographs and use of website
- eBullying / Cyber-bullying procedures
- Their role in providing e-Safety education for students

School staff have the specific power under the Education and Inspections Act 2006 (which has been increased by the Education Act 2011) to search for and, if necessary, delete inappropriate images or files on students' electronic devices, including mobile phones, iPads and other tablet devices, where they believe there is a 'good reason' to do so.

When deciding whether there is a good reason to examine or erase data or files on an electronic device, staff must reasonably suspect that the data or file in question has been, or could be, used to:

- Cause harm, and/or

- Disrupt teaching, and/or
- Break any of the school rules

If inappropriate material is found on the device, it is up to the staff member in conjunction with a member of the senior leadership team to decide whether they should:

- Delete that material, or
- Retain it as evidence (of a criminal offence or a breach of school discipline), and/or
- Report it to the police

Any searching of students will be carried out in line with the DfE's latest guidance on screening, searching and confiscation.

Any complaints about searching for or deleting inappropriate images or files on students' electronic devices will be dealt with through the school complaints procedure.

4. How will complaints regarding e-Safety be handled?

The school will take all reasonable precautions to ensure e-Safety. However, owing to the international scale and linked nature of Internet content, the availability of mobile technologies and speed of change, it is not possible to guarantee that unsuitable material will never appear on a school computer or mobile device. Neither the school nor the Local Authority can accept liability for material accessed, or any consequences of Internet access.

Staff and students are given information about infringements in use and possible sanctions. Sanctions available include:

- interview / counselling by tutor / Pastoral and Progress Leader / E-Safety Co-ordinator / SLT / Principal
- informing parents or carers
- removal of Internet or computer access for a period, [which could ultimately prevent access to files held on the system, including examination coursework]
- referral to LA / Diocese / Police
- range of sanctions in accordance with our Anti-Bullying Policy and Behaviour Management Policy

Our E-Safety Coordinator acts as first point of contact for any complaint. Any complaint about staff misuse is referred to the Principal. Complaints of cyber-bullying are dealt with in accordance with our Anti-Bullying Policy. Complaints related to child protection are dealt with in accordance with school / LA child protection procedures.

Decisions on appropriate use of content, images, communications or behaviour shall be consistent with the School's other Safeguarding policies.

5. Cyberbullying

In addition to the difficulties in managing the use of social media services, a further challenge that arises from the spread of ICT and social networking media is cyberbullying which has been defined as *"any use of information and communications technology to support deliberate and hostile attempts to hurt, upset or embarrass another person".*

Cyberbullying might include offensive emails, email threats, posting blogs and leaving comments on social networking sites, propagating defamatory gossip about employees, threats or offensive

comments sent to a person's mobile phone via SMS text-messages, harassment by email or sharing a person's private data online.

The school and its employees have a duty of care to ensure that cyberbullying is not tolerated within this community. Any breach of this policy will result in the school's disciplinary procedure being invoked.

In relation to a specific incident of cyberbullying, the school will follow the processes set out in the Anti-Bullying Policy / Behaviour Management Policy. Where illegal, inappropriate or harmful material has been spread among pupils, the school will use all reasonable endeavours to ensure the incident is contained.

The Senior Designated Safeguarding Lead will consider whether the incident should be reported to the police if it involves illegal material, and will work with external services if it is deemed necessary to do so.

Appendix A

E-SAFETY – GUIDANCE FOR STAFF

Refer to: Staff Code of Conduct

School Systems – Code of Practice

Information Communication Technology

All staff are reminded of their responsibility to follow the 'Code of Practice' outlined in the staff handbook.

Security of Systems

Staff are provided with individual access permissions on all systems required to fulfil their duties (SIMS/Portal/FMS etc.) Security of the schools systems is essential and staff are reminded to follow the network password policy detailed below:

Your network password must contain at least 5 characters and should include at least 1 upper case letter, 1 lower case letter and 1 number.

This password is unique to the individual and must never be shared with anyone

The individual password should be changed at least once per year.
Staff passwords should not be written down.

Staff using work devices outside school

Staff must ensure that their work device is secure and password-protected, and that they do not share their password with others. They must take all reasonable steps to ensure the security of their work device when using it outside school. Any USB devices containing data relating to the school must be encrypted.

If staff have any concerns over the security of their device, they must seek advice from the System Administrator.

Access to the Internet

The school's access to the internet is limited to 'acceptable use' within an educational establishment. The school is protected by systems to ensure that the school's safeguarding responsibilities are met and to reduce the risk of viruses entering the network. Scanning services ensure that the system remains secure and when they come across a website which comes into categories that pose risk to the community, then this will be blocked.

Access to the internet at work is for professional use only.

Social Media

Staff should be aware that 'online conduct' should not differ from 'offline professional conduct' and that staff must ensure that behaviour does not cause offence nor bring the school into disrepute. Staff are reminded of the following:

"Everything you share on a social networking site could potentially end up in the worldwide public domain and be seen or used by someone you did not intend, even if it appears to be 'private' or is on a closed profile group."

If you use social media irresponsibly, then you risk breaking school procedures and this is likely to be referred to the School's Disciplinary Procedures.

The basic premise, therefore, is that employees need to exercise common sense and to realise that what they write on social networking sites is essentially in the public domain.

Staff are reminded of the potential dangers of using online media. Staff should not disclose personal details or whereabouts, disclosing information unintentionally, choose online 'friends' carefully, disclosing information about colleagues or the school, including photographs and/or videos. Staff should not use social networking sites in such a way that brings the school into disrepute, e.g. through posting derogatory remarks about the organisation, colleagues or managers.

Staff must be aware of the risk in posting information themselves on social networking sites such as Facebook as this is accessible to the public, including, potentially, their employer and the wider community. The employer and community are therefore in a position to access a range of material relating to the employees' behaviour outside of their work and that carries the potential to affect their reputation and dignity within work.

The school does not look at Facebook or other social networking sites of its employees as a matter of course, as it does not want to prescribe how employees should behave in their private life. For the organisation, the main and overarching issue is that employees do not behave in such a way as to bring the organisation/profession into disrepute.

Relationships at work

Social networking sites tend to blur traditional relationship boundaries, individuals may have a large number of 'friends' on their Facebook site – some of which may not actually be friends in the conventional sense of the word, and indeed they may never have actually met. Within the workplace, social networking sites can disrupt traditional boundaries and relationships between employees, students, parents and the wider community.

Staff are reminded that they must endeavour to protect their professional authority by ensuring that professional boundaries are completely intact. Staff must not include 'students' as 'friends' within social networks. It is also inadvisable to include 'parents' and 'governors' as 'friends' within your network. Students can become confused by the blurring of boundaries and it is a member of staff's responsibility to ensure that their conduct is professional at all times.

Staff are provided with email addresses for professional use; this means of communication is acceptable and staff should ensure that the following terminology is always used:

Title:	Teaching Staff must refer to themselves by their title e.g. 'Mr', 'Miss' etc.
Content:	The content of all emails should relate directly to the academic or pastoral responsibilities for that student/parent.
Address:	The school address should be supplied for any written communication i.e. name@cncs.co.uk or the full written address The Upper Drive, Hove, BN3 6ND
Mobile:	Staff must not share their private mobile numbers with students.
Phones	Staff with school mobiles are able to support the community with additional communication systems.

First names should not be used within any professional communication with parents or students.

Appendix B

Student Acceptable Use Policy

All students must follow the conditions described in this policy when using school ICT networked resources including: Internet access, the school Learning Platform both in and outside of school. Breaking these conditions may lead to:

- Withdrawal of the student's access,
- Close monitoring of the students network activity,
- Investigation of the students past network activity,
- In some cases, criminal prosecution.

Students will be provided with guidance by staff in the use of the resources available through the schools network. School staff will regularly monitor the network to make sure that it is being used responsibly. The school will not be responsible for any loss of data as a result of the system or student mistakes in using the system. Use of any information obtained via the network is at the student's own risk.

Students are also reminded that any unacceptable activity on the internet (at school or outside of school) that brings the school, members of staff or other students into disrepute may result in disciplinary action in line with our Behaviour Management policy.

Conditions of Use

Student access to the networked resources is a privilege, not a right. Students will be expected to use the resources for the educational purposes for which they are provided. It is the personal responsibility of every student to take all reasonable steps to make sure they follow the conditions set out in this Policy. Students must also accept personal responsibility for reporting any misuse of the network to the Network Manager.

ACCEPTABLE USE

Students are expected to use the network systems in a responsible manner. It is not possible to set a complete set of rules about what is, and what is not, acceptable. All use however should be consistent with the school ethos and code of conduct. The following list does provide some examples that must be followed:

1	I will not create, send or post any material that is likely to cause offence or needless anxiety to other people or bring the school into disrepute.
2	I will use appropriate language – I will remember that I am a representative of the school on a global public system. Illegal activities of any kind are strictly forbidden.
3	I will not use language that could stir up hatred against any ethnic, religious or other minority group.
4	I realise that files held on the school network will be regularly checked by the Network Manager or other members of staff.
5	I will not reveal any personal information (e.g. home address, telephone number) about myself or other users over the network.
6	I will not trespass into other users' files or folders.

7	I will not share my login details (including passwords) with anyone else. Likewise, I will never use other people's username and password.
8	I will ensure that if I think someone has learned my password then I will change it immediately and/or contact the Network Manager.
9	I will ensure that I log off after my network session has finished.
10	If I find an unattended machine logged on under other users username I will not continuing using the machine – I will log it off immediately.
11	I understand that I am will not be allowed access to unsupervised and/or unauthorised chat rooms and should not attempt to gain access to them.
12	I am aware that e-mail is not guaranteed to be private. Messages supporting of illegal activities will be reported to the authorities. Anonymous / unnamed messages are not permitted.
13	I will not use the network in any way that would disrupt use of the network by others.
14	I will report any accidental access to other people's information, unsuitable websites or being sent inappropriate materials that make me feel uncomfortable to the Network Manager.
15	I will not introduce "USB drives" or other portable devices into the network without having them checked for viruses.
16	I will not attempt to visit websites that might be considered inappropriate or illegal. I am aware that downloading some material is illegal and the police or other authorities may be called to investigate such use.
17	I will not download and/or install any unapproved software, system utilities or resources from the Internet.
18	I realise that students under reasonable suspicion of misuse in terms of time, activity or content may have their usage closely monitored or have their past use investigated.
19	I will not receive, send or publish material that violates copyright law. This includes materials sent / received using Video Conferencing or Web Broadcasting.
20	I will not attempt to harm or destroy any equipment, work of another user on the school network, or even another website or network connected to the school system.
21	I understand that unapproved system utilities and executable files are not allowed in my work areas or attached to e-mails.
22	I agree to comply with the acceptable use policy of any other networks that I access.

UNACCEPTABLE USE

Examples of unacceptable use include, but are not limited to:

- Logging in with another person's user ID and password, or using a machine left unattended, but logged in by another user.
- Creating, transmitting, displaying or publishing any material (text, images or sounds) that is likely to harass, cause offence, inconvenience or needless anxiety to any other person.
- Unauthorised access to data and resources on the school network system that belong to other "users".
- User action that would cause:
  - Corruption or destruction of other users' data,

- Violate the privacy or dignity of other users,
- Intentionally waste time or resources on the school network or elsewhere.

NETWORK SECURITY

If you discover a security problem, for example being able to access other user's data, you must inform the System Administrator immediately and not show it to other users. Students identified as a security risk will be denied access to the network.

Parents

Parents are expected to:

- Notify a member of staff or the Principal of any concerns or queries regarding this policy
- Ensure their child has read and understood the CNCS Code of Practice for the school's ICT systems and internet which can be viewed in the Computing and ICT Policy

Parents can seek further guidance on keeping children safe online from the following organisations and websites:

- What are the issues?, UK Safer Internet Centre: https://www.saferinternet.org.uk/advice-centre/parents-and-carers/what-are-issues
- Hot topics, Childnet International: http://www.childnet.com/parents-and-carers/hot-topics
- Parent factsheet, Childnet International: http://www.childnet.com/ufiles/parents-factsheet-09-17.pdf

Key Personnel in relation to this Policy:

Dr James Kilmartin – Principal
Claire Jarman – Designated Safeguarding Lead
Cindy Goddard - Child Protection Officer
Andy Hart – E-Safety Co-ordinator

Linked Policies:

Anti-Bullying Policy

Behaviour Management Policy

Safeguarding and Child Protection Policy