Methodist College Belfast
e-Safety & ICT Acceptable Use Policy

Rationale

Mobile phones include many additional functions such as an integrated camera, video recording capability, instant messaging, mobile office applications and mobile access to the internet. These allow immediate access to email, searching for information on the internet and other functions such as access to social networking sites e.g. Facebook, Twitter and blogging sites.

We recognise and value the increasingly wide opportunities that information technology provides to our staff and pupils. Whilst it is our aim that all members of our school community avail as fully as possible of this technology we also appreciate the need for safeguards to be in place. Young people have many opportunities to benefit from what are becoming very sophisticated hand-held devices outside school. However it should be recognised that at present their usefulness in the school context is limited.

Aim

To highlight the responsibility of the College, staff, governors and parents to mitigate risk through reasonable planning and actions. The e-Safety and ICT Acceptable Use Policy covers not only Internet technologies but also electronic communications via mobile phones, games consoles and wireless technology both inside and outside school.

Objectives

e-Safety in the school context:

- is concerned with safeguarding children and young people in the digital world;
- emphasises learning to understand and use new technologies in a positive way;
- is less about restriction and focuses on education about the risks as well as the benefits so that users feel confident online;
- is concerned with supporting pupils to develop safer online behaviours both in and out of school; and
- is concerned with helping pupils recognise unsafe situations and how to respond to risks appropriately.

Definitions (DENI circular 2013/25)

1. **e-Safety** is short for electronic safety.
2. **Internet Filtering** - Improved Websense filtering will give schools the flexibility to control and develop their own Internet Filtering Policy. Individual schools may now select to fully delegate

management of their filtering policy to a nominated member of staff by signing up to C2k delegated filtering access. This nominated user will receive additional training for this responsibility and can further amend the local filtering policy to the needs and demands of the school. This is in direct response to feedback from schools, who wish to access more internet sites to enhance teaching and learning. However there are a number of agreed locked down sites that can never be overridden by the local school policy.

3. **Meru Wireless** - Meru Wi-Fi will provide increased wireless coverage and improved speed. Meru supports multiple devices and school controlled secure guest access and allows schools to plan for and implement a further purchase by the school or/and a 'Bring Your Own Device' policy.
4. **Cloud Storage** - Data and information will be stored on the Cloud in the new service and no longer in the school itself. This means it can be securely accessed from any location removing the need to carry data and files on insecure data pens and portable devices.

Roles and Responsibilities

Principal

- The Principal 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 ICT co-ordinator.
- The Principal and the Designated Teacher for Child Protection should be aware of the procedures to be followed in the event of a serious e-safety allegation being made against a member of staff.

ICT Manager

- Ensures that the College's technical infrastructure is not open to misuse or malicious attack and meets required e-Safety requirements and guidance issued by the Department of Education, both on C2k and legacy equipment
- Ensures that users may only access the networks and devices through properly enforced passwords, which are changed regularly
- Regularly monitors the use of the network / internet / VLE / remote access and email in order that any misuse is reported to the e-Safety Coordinator
- Ensures that any software/systems are implemented/uploaded in line with school policy

Head of Pastoral Care

- Takes day to day responsibility for e-safety issues, convenes the E-Safety Group which establishes and reviews the College's e-safety policies / documents
- Ensures that all staff and pupils are aware of the procedures that need to be followed in the event of an e-Safety incident taking place.
- In conjunction with the Head of ICT and Deputy Heads of Pastoral Care, ensures training and advice for staff and pupils is provided
- As Designated Teacher, should be trained in e-safety issues and be aware of the potential for serious child protection/safeguarding 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

Heads of Form

- Will investigate and deal with any reports of misuse/attempted misuse of the network or electronic media
- HoFs will deal with any reports of cyber-bullying (See Anti-Bullying Policy)

Teachers and support staff

are responsible for ensuring that:

- they have an up to date awareness of e-safety matters and of the current school e-safety policy and practices
- they have read, understood and signed the Staff Acceptable Use Policy (AUP) – see Appendix 2
- they report any suspected misuse or problem to the relevant HoF
- all digital communications with pupils/parents/carers should be on a professional level and only carried out using official school systems
- e-safety issues are embedded in all aspects of the curriculum and other activities
- pupils understand and follow the e-safety and acceptable use policy
- pupils 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, ensuring the suitability of materials to be used in lessons and other school activities (where allowed).

Pupils

are responsible for using the College's technology systems in accordance with the Pupil Acceptable Use Policy – see Appendix 3. They need to

- have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations
- 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. They should also 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 College's e-Safety Policy covers their actions out of school, if related to their membership of the school (though the College cannot police the internet when the students are in the care of their parents/guardians).

Parents/Guardians

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

- digital and video images taken at school events
- access to parents' sections of the website

- their children's personal devices in the College
- use of social media

Professional Development for Teachers

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:

- E-safety information will be made available to staff at the beginning of each academic year. This will be regularly updated, disseminated and reinforced. Where necessary training will also be provided during the academic year.
- All new staff should receive e-safety information as part of their induction programme, ensuring that they fully understand the school e-safety and Acceptable Use policy.
- The Pastoral staff will receive updates through attendance at external training events and by reviewing guidance documents released by relevant organisations.

Education of Pupils

Whilst regulation and technical solutions are very important, their use must be balanced by educating pupils to take a responsible approach. The education of pupils in e-safety is therefore an essential part of the College's e-safety provision. Pupils need the help and support of the school to recognise and avoid e-safety risks and build their resilience.

E-safety should be a focus in all areas of the curriculum and staff should reinforce e-safety messages across the curriculum. The e-safety curriculum should be broad, relevant and provide progression, with opportunities for creative activities and will be provided in the following ways:

- A planned e-safety curriculum will be provided as part of ICT classes
- Key e-safety messages will be reinforced as part of a planned programme of assemblies (e.g. Safe Internet Day)
- Pupils will be taught to be critically aware of the materials/content they access on-line and be guided to validate the accuracy of information
- Pupils will be taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet
- Pupils will be helped to understand the need for the Pupil Acceptable Use policy and encouraged to adopt safe and responsible use both within and outside school
- Staff will act as good role models in their use of digital technologies, the internet and mobile devices
- In lessons where internet use is pre-planned, pupils will be guided to sites checked as suitable for their use

Cyberbullying

Bullying, intimidation and harassment are not new in society; however bullying via electronic methods of communication both in and out of school represents a new challenge for schools to manage.

Staff should be aware that pupils may be subject to cyber bullying via electronic methods of communication both in and out of school. This form of bullying should be considered within the College's overall Anti-bullying Policy and pastoral services as well as the eSafety policy.

Whilst cyber-bullying may appear to provide anonymity for the bully, most messages can be traced back to their creator and pupils should be reminded that cyber-bullying can constitute a criminal offence. While there is no specific legislation for cyber-bullying, the following may cover different elements of cyber-bullying behaviour:

- Protection from Harassment (NI) Order 1997
http://www.legislation.gov.uk/nisi/1997/1180
- Malicious Communications (NI) Order 1988
http://www.legislation.gov.uk/nisi/1988/1849
- The Communications Act 2003
http://www.legislation.gov.uk/ukpga/2003/21

It is important that pupils are encouraged to report incidents of cyber-bullying to both the school and, if appropriate, the PSNI to ensure the matter is properly addressed and the behaviour ceases.

These guidelines are intended to help a school make explicit the expectations of the school on pupil use of mobile phones and the restrictions which are placed on their use in school and on school grounds. The guidelines sit alongside the Acceptable Use Policy which all pupils sign and is shared with parents and carers. They also give clear guidance to staff, pupils and parents about the consequences for breaches of the guidelines.

Dealing with breaches of the e-Safety and Acceptable use policy

Misuse of a mobile device will be dealt with according to College Rules, with the response being proportionate to the severity of the misuse.

The Vice Principal (Pastoral) will deal with serious incidents of misuse, particularly where cyberbullying is suspected to have taken place.

Staff should keep good records of cyber-bullying incidents, following the College's Anti-Bullying Policy, to ensure consistency in their investigations, support and sanctions.

Pupils should be aware that serious misuse may lead to the confiscation of their mobile device, communication with parents and the imposition of other sanctions up to and including exclusion from the College. If the offence is criminal in nature it will be reported to the PSNI.

The Principal or a designated staff member will have the right to view files stored in confiscated equipment and will seek the cooperation of parents in deleting any files which are in clear breach of these Guidelines unless these are being preserved as evidence.

If required evidence of the offence will be preserved, preferably by confiscation of the device and keeping it secure or by taking photographs of the screen.

Advice can be sought from the EA(BELB) Safeguarding Team and/or the PSNI.

Communication of the e-Safety Policy

<u>Communication with pupils</u>

- All users will be updated about the e-safety and AUP annually in Assemblies

- An e–Safety training programme will be established across the school to raise the awareness and importance of safe and responsible internet use amongst pupils.
- An e–Safety module will be included in the Form 1 ICT programme covering both safe school and home use.
- e-Safety rules or copies of the student Acceptable Use Policy will be posted on the school website and College intranet.
- Safe and responsible use of the Internet and technology will be reinforced across the curriculum and subject areas.
- Particular attention to e-Safety education will be given where pupils are considered to be vulnerable.

Communication with staff

It is important that all staff feel confident to use new technologies in teaching and the College's e–Safety Policy will only be effective if all staff subscribe to its values and methods.

- The e–Safety Policy will be formally provided to and discussed with all members of staff.
- Up-to-date and appropriate staff training in safe and responsible Internet use, both professionally and personally, will be provided for all members of staff.
- Staff who manage filtering systems or monitor ICT use will be supervised by the Senior Leadership Team and have clear procedures for reporting issues.
- The College will highlight useful online tools which staff should use with children in the classroom. These tools will vary according to the age and ability of the pupils.
- All members of staff will be made aware that their online conduct out of school could have an impact on their role and reputation within school. Civil, legal or disciplinary action could be taken if they are found to bring the profession or institution into disrepute, or if something is felt to have undermined confidence in their professional abilities. Discretion and professional conduct is essential.

Communication with parents

- This policy will be emailed to all parents annually
- An E-safety briefing is given to all Form 1 parents

Links to other policies

This policy should be read in conjunction with the other policies of the college, in particular those concerning:

Child Protection
Positive Behaviour
Anti-Bullying

Revised: June 2018

Next revision: June 2019. This policy will be reviewed annually by the E-safety Group

Appendix 1 Legal Framework

Notes on the legal framework

This section is designed to inform users of potential legal issues relevant to the use of electronic communications.

Many young people and indeed some staff use the Internet regularly without being aware that some of the activities they take part in are potentially illegal. Please note that the law around this area is constantly updating due to the rapidly changing nature of the internet.

Public Order (N.I.) 1987

This Act makes it a criminal offence to stir up hatred or arouse fear. Fear and Hatred both mean fear/hatred of a group of persons defined by reference to religious belief, colour, race, sexual orientation, disability, nationality or ethic or national origins

Criminal Justice (No2) (N.I.) Order 2004

Commonly referred to as N.I. 'Hate Crime' legislation. This empowers courts to impose tougher sentences when an offence is aggravated by hostility based on the victims actual or presumed religion, race, sexual orientation or disability.

Protection of Children (N.I.) Order 1978

It is an offence to take, permit to be taken, make, possess, show, distribute or advertise indecent images of children in Northern Ireland. A child for these purposes is anyone under the age of 18. Viewing an indecent image of a child on your computer means that you have made a digital image. An image of a child also covers pseudo-photographs (digitally collated or otherwise). This can include images taken by and distributed by the child themselves (often referred to as "Sexting"). A person convicted of such an offence may face up to 10 years in prison.

Sexual Offences (N.I.) order 2008

The offence of grooming is committed if you are over 18 and have communicated with a child under 16 at least twice (including by phone or using the Internet). It is an offence to meet them or travel to meet them anywhere in the world with the intention of committing a sexual offence.

Causing a child under 16 to watch a sexual act is illegal, including looking at images such as videos, photos or webcams, for your own gratification.

Obscene Publications Act 1959 and 1964

Publishing an "obscene" article is a criminal offence. Publishing includes electronic transmission

Protection from Harassment (N.I.) Order 1997

Article 3.This legislation can be considered where a person is pursuing a course of conduct which amounts to harassment. This includes alarming a person or causing a person distress. This course of conduct must be on more than one occasion

Communications Act 2003 (section 127)

Sending by means of the Internet a message or other matter that is grossly offensive or of an indecent, obscene or menacing character; or sending a false message by means of or persistently making use of the Internet for the purpose of causing annoyance, inconvenience or needless anxiety is guilty of an offence liable, on conviction, to imprisonment. This wording is important because an offence is complete as soon as the message has been sent: there is no need to prove any intent or purpose.

Data Protection Act 1998

The Act requires anyone who handles personal information to notify the Information Commissioner's Office of the type of processing it administers, and must comply with important data protection principles when treating personal data relating to any living individual. The Act also grants individuals rights of access to their personal data, compensation and prevention of processing.

The Computer Misuse Act 1990 (sections 1 - 3)

Regardless of an individual's motivation, the Act makes it a criminal offence to:
• gain access to computer files or software without permission (for example using someone else's password to access files);
• gain unauthorised access, as above, in order to commit a further criminal act (such as fraud); or
• impair the operation of a computer or program (for example caused by viruses or denial of service attacks).

UK citizens or residents may be extradited to another country if they are suspected of committing any of the above offences.

Malicious Communications Act 1988 (section 1)

This legislation makes it a criminal offence to send an electronic message (email) that conveys indecent, grossly offensive, threatening material or information that is false; or is of an indecent or grossly offensive nature if the purpose was to cause a recipient to suffer distress or anxiety.

Copyright, Design and Patents Act 1988

Copyright is the right to prevent others from copying or using his or her "work" without permission. The material to which copyright may attach (known in the business as "work") must be the author's own creation and the result of some skill and judgement. It comes about when an individual expresses an idea in a tangible form. Works such as text, music, sound, film and programs all qualify for copyright protection. The author of the work is usually the copyright owner, but if it was created during the course of employment it belongs to the employer.

It is an infringement of copyright to copy all or a substantial part of anyone's work without obtaining the author's permission. Usually a licence associated with the work will allow a user to copy or use it for limited purposes. It is advisable always to read the terms of a licence before you copy or use someone else's material.

It is also illegal to adapt or use software without a licence or in ways prohibited by the terms of the software licence.

Regulation of Investigatory Powers Act 2000

The Regulation of Investigatory Powers Act 2000 (RIPA) regulates the interception of communications and makes it an offence to intercept or monitor communications without the consent of the parties involved in the communication. The RIP was enacted to comply with the Human Rights Act 1998.

The Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000, however, permit a degree of monitoring and record keeping, for example, to ensure communications are relevant to school activity or to investigate or detect unauthorised use of the network. Nevertheless, any monitoring is subject to informed consent, which means steps must have been taken to ensure that everyone who may use the system is informed that communications may be monitored.

Covert monitoring without informing users that surveillance is taking place risks breaching data protection and privacy legislation.

Criminal Justice and Immigration Act 2008

Sec 62-68 Includes the Coroners and Justice Act. It is an offence to possess a drawing or painting which depicts a child in an indecent pose or participating in an indecent act.

Section 63 offence to possess "extreme pornographic image"

63 (6) must be “grossly offensive, disgusting or otherwise obscene”
63 (7) this includes images of “threats to a person life or injury to anus, breasts or genitals, sexual acts with a corpse or animal whether alive or dead” must also be “explicit and realistic”. Penalties can be up to 3 years imprisonment.

Education and Inspections Act 2006

Education and Inspections Act 2006 outlines legal powers for schools which relate to Cyberbullying/Bullying:
• Principals have the power “to such an extent as is reasonable” to regulate the conduct of pupils off site.
• School staff are able to confiscate items such as mobile phones etc when they are being used to cause a disturbance in class or otherwise contravene the school behaviour/anti bullying policy.

DENI Circular 2016 / 27 – Online Safety (Issued 1/12/16

Appendix 2

Methodist College Belfast
ICT Acceptable Use Policy for Staff

Rationale

The purpose of this document is to offer guidance about the use of ICT resources available to staff. All staff must read the information contained in this document and be familiar with it before using the ICT resources in the College.

In the context of this document ICT refers to computer based systems used in the learning and teaching that takes place in the College and any use of ICT resources related to extra curricular activities or field trips.

Guidelines for Staff on the Use of ICT Resources

All staff are expected to use the school computer systems and ICT resources in a manner that befits the ethos of the College. They must not bring the name of the College or themselves into disrepute.

1a. Use of ICT Resources in Methodist College

The College has ten main computer rooms. The workstations in these rooms are Microsoft Windows based systems and are linked to a scanner and networked printer. There is also a multimedia computer suite with networked Apple iMac workstations. Workstations are also situated in the Library, 6th Form Study Floor a number of departments and staffrooms throughout the College and the administration offices. Internet and multimedia capability are available on all networked computers. Laptops and iPads are also available for use in classrooms. Each member of staff has been provided with an iPad.

1b. Booking of ICT Resources

A Resource Booking System is available. Members of staff can book various rooms and ICT equipment throughout the College. This can be accessed via the custom tab in My School. Please note that in the first instance certain rooms may need to be booked via the Premises Department. This is clearly indicated on the room entry on the electronic booking form.

Each classroom in the College is equipped with a workstation, data projector, iPad connection and screen. Interactive whiteboards are also located in various classrooms throughout the College.

1c. ICT Help Desk

In order to provide ICT support, the MCB Help Desk facility is available to Staff. This can be accessed via the custom tab in My School and also the school intranet site. All Staff are required to use this as their first point of contact when an ICT issue arises. Please ensure that all the required information is entered on the request form to ensure a swift and timely response to any request. In exceptional circumstances it is possible to contact ICT support in the following ways.

Telephone: **244**, or email **ICT Support** from the Outlook email distribution list.

- When using the ICT resources
  - Never try to copy computer software from the school computer systems. (This may be theft).
  - Do not violate copyright laws.
  - Do not intentionally waste ICT resources
  - Never try to bypass or hack the security systems of the computer rooms or the computer systems. This includes the bypassing of any website filtering services to access blocked web sites.
  - If specific computer software needs to be installed either locally or on the network the IT Manager must be informed to ensure no contravention of the licensing laws occurs and to prevent software conflicts.
  - Never tamper with the cables and connections on the workstations
  - Always report any damage to ICT equipment or computer rooms to a member of IT support immediately.
  - Food and drink must not be consumed in the computer rooms *at any time*.
- Members of staff must take care in their use of portable devices including iPads, pen drives or external hard drives.
  - Pastoral or confidential information must not be stored on portable devices.
  - Confidential information that needs to be transferred on a portable device must have a secure password to protect its contents.
  - All portable devices which are brought onto College premises, even if they are the personal property of staff, must not have material stored on them which would contravene the regulations and ethos of the College, even if the material is not for use in the College.
  - No software of any type should be stored on any portable device for the purpose of installation on any school device without the consent of the IT Manager.
  - Do not use a removable device for viewing illegal or unacceptable media of any type in the College.

2. Use of the C2K Network and Email Accounts

All staff are allocated a C2K personal email account and area for the storage of documents which they are responsible for maintaining**.** Computer file storage areas and removable storage media of any kind may be reviewed by the IT Manager at any time.

- Members of staff should use their C2K email account for corresponding with pupils and parents as this is filtered and monitored.
- Any emails should be restricted to matters relating to College business only.
- Staff should never use a personal email address for communicating with pupils or parents.
- SPAM and unsolicited emails are automatically filtered out so that the recipient does not receive them. Users are now their own mail managers and can request their release by contacting the CAPITA helpdesk on 08706011666.

- For the most part staff work areas and emails will be treated as being private except where there is a clear reason for the IT Manager or an outside agency to review them with the permission of the Principal.
- All usernames and passwords must be kept private.
    - Do not permit any other member of staff or a pupil to access the network using your username or password.
    - Users will be forced to change their password every 120 days.
    - No one is permitted to use a computer logged on with another person's username.
    - Do not trespass in other users' folders, work or files.
- When using ICT resources members of staff must not:
    - Send or display offensive messages or pictures.
    - Send or play offensive sound recordings.
    - Use obscene language either verbally or via an electronic device.
    - Harass, insult or attack others on line
- Any electronic communication containing unacceptable material should be reported to the Principal or a Vice-Principal immediately.
    - Do not forward or delete the material until the Principal or Vice-Principal has seen it.
    - If a member of staff accidentally accesses unacceptable material via the College network they should report it immediately to the Principal.
- When sending emails
    - Names of pupils should never be typed into the subject line of emails.
    - Only open attachments to emails if they come from a known and trusted sender as attachments may contain viruses or other programs that could destroy files or software.
- Care should be taken when using the data projector in class.
    - SIMS registers should not be projected onto the screen.
    - MS Outlook should not be open when using the projectors to ensure that confidential information contained in emails is not shown on the bottom of the screen.
- Before photographs or digital recordings are taken, staff and volunteers should read the *Use of Images* section in the Staff Guide and also check if a parent/guardian has given permission for images of their child to be published either inside and/or outside the College.
    - There is an <u>easy way to check for this permission</u> on SIMs
        - Reports (top left area)
        - Run Report
        - Focus
        - Student
        - *Either* Parental Consent Photograph *or* <u>even better</u> Parental Consent NO Photo

3. Internet Access

All internet access through the College's C2K network is filtered. Internet browsing history is monitored and can be recalled at any time at the request of the Principal.

Be aware that the Blue Tooth facility on your mobile or iPad could inadvertently pick up file transfers by pupils if it is switched on during the school day or whilst on a school trip.

4. Social Networks & Cyber Safety Advice

Whilst Social Networking sites are not accessible through the C2K System, it is advisable for staff to adhere to the guidance listed below when using Social Media.

- Ensure that social networking account privacy settings are at “friends only” or “protected”.
- Do not accept friend requests from pupils, past or present or request to be friends with pupils.
- Do not post private details such as home address, mobile or home telephone numbers or other personal details.
- Be careful about the content and nature of any material that is posted on social networking sites.
- Do not post anything online that could bring the College into disrepute.
- Do not post or tweet opinions or comments about individuals as it could cause offence.

Remember

- You are not anonymous online; all correspondence can be sourced through the computer’s IP address.
- Photos or comments that are posted or tweeted can be forwarded on to others by friends or followers without your permission.
- There could be serious consequences to the use of social networks.

Any requests for further information in relation to any of the information contained in this Acceptable Use Policy should be addressed to:

Mr F. Cassidy

IT Manager
fcassidy664@c2kni.net

02890 205205

Appendix 3

Methodist College Belfast
ICT Acceptable Use Policy for Pupils

1. Introduction

The purpose of this document is to ensure that pupils understand the guidelines for acceptable use of ICT Resources and to ensure that staff, pupils and parents can work together to effectively use ICT to enhance the learning experience.

In the context of this document ICT refers to computer based systems and any ICT resources related to extra curricular activities or field trips. It applies to all platforms, including desktops, laptops, tablet devices and mobile phones.

Pupils must ensure that their use of the College ICT resources is appropriate at all times. All users are required to comply with school regulations and not to bring the name of the College or themselves into disrepute.

2. The C2K Network and Email

All pupils are allocated a C2K personal email account and area for the storage of documents which they are responsible for maintaining.

SPAM and unsolicited emails are automatically filtered out so that the recipient does not receive them. Users are notified of these messages and can request their release from the IT Manager by forwarding the notification email on to him.

Pupils should be aware that files stored on the C2K network are not private. Staff may review files and communications to ensure that pupils are using the network responsibly.

3. Internet Access

All internet access through the College's C2K network is filtered and monitored and can be recalled at any time at the request of the Principal.

Any electronic communication containing unacceptable material should not be forwarded or deleted but must be reported to a member of staff or the IT Manager immediately.

If a pupil accidentally accesses unacceptable material via the College network they should report it immediately to their teacher or the IT Manager.

3.Use of Printers

Pupils will be given some printer credits at the start of each year. Once these are used up, more credits can be purchased from the ICT Support Team in K Block

Pupils should only use the school printers to produce school-related materials.

Pupils should try to reduce the number of items they print in an effort to reduce waste and the use of paper in the College. They should avoid using large areas of block colour or black ink in what they create to minimise the use of printer ink.

4. Computer Access Outside School Hours

One computer room, usually K9, is open for pupil use from 8.00 am until 8.40 am each morning, from 12.20 to 1.20 on Monday – Thursday and 12.35 – 1.05 on a Friday and after school from 3.20 p.m to 4.25 p.m. Monday to Thursday and from 3.00 pm to 4.25pm on Friday.

K8 and the Study Floor computer room are available for 6th Form use subject to the rooms not being used for timetabled classes.

Pupils can have access to their e-mail, Fronter and a range of other material from home through the My School portal. Google - *My School C2K.* Use your school C2K username and password to access My School.

5. Pupil Guidelines On The Use of ICT Resources

Pupils are responsible for good behaviour and appropriate use of College ICT resources and are expected to use them in a manner that befits the ethos of the College. Access to any ICT resource is a privilege, not a right.

- Pupils must ensure that their use of the College Computer Network is appropriate at all times.
- When using ICT resources pupils must not:
- *Send or display offensive messages or pictures.*
- *Send or play offensive sound recordings.*
- *Use obscene language either verbally or via an electronic device.*
- *Harass, insult or attack others on line.*
- All usernames and passwords must be kept private. Do not permit anyone else to access the network using your username or password. No one is permitted to use a computer logged on with another person's username or trespass in other users' folders, work or files.
- Only open attachments to emails if they come from a known and trusted sender as attachments may contain viruses or other programs that could destroy files or software.
- Never try to bypass or hack the security systems of the computer rooms or the computer systems. This includes the bypassing of any website filtering services to access blocked web sites.
- Never try to copy computer software from the school computer systems. (This may be theft).
- No software of any type should be stored on any removable media for the purpose of installation on any school device without the consent of the IT Manager.
- Do not violate copyright laws.
- Do not waste ICT resources.
- **Never bring a mobile phone, iWatch, iPad, MP3 player or any electronic device into an exam room as this could result in disqualification.**
- Do not use external removable devices for viewing illegal or unacceptable media of any type.
- Computer file storage areas and removable storage media of any kind may be reviewed by the IT Manager at any time.
- Food and drink are not allowed to be consumed in the computer rooms ***at any time***.
- Never tamper with the cables and connections on the workstations
- Always report any damage to ICT equipment or computer rooms to a teacher or IT Manager immediately.

6. Advice on the use of College iPads.

The College currently has up to 60 iPads available as class sets for classroom use. The use of tablet devices for research, sharing work and specific applications is set to increase. Pupils should follow this advice when they use the College iPads.

- Log on to the internet using your set C2K username and password.
- Ensure that you are fully logged off from all applications before you return the iPad.
- Remember your use of the iPad can be traced just as a normal school computer.
- Do not tamper with any existing settings on the iPad.
- If you wish to store the work you create, you should do this on a Cloud based location such as Dropbox, GoogleDrive or the Onedrive
- To do this, you will need to create your own account. Create your account using your C2K user name. The free to access storage in such Cloud locations should provide you with enough space for school use.
- If you have been using photographs and/or video, you should delete these from the iPad when your project is complete.
- If there are specific apps that you feel will help your learning, please speak to your teacher or the ICT manager who may be able to purchase them for future use.

7. Cyber Safety Advice

Pupils are not permitted to access social networking sites via the College network. However, the following guidelines are suggested to ensure pupil safety and security when using these websites outside school.

Do not give out or post personal information online – report it to a trusted adult and/or use this website https://www.thinkuknow.co.uk/
Make sure that social networking account privacy settings are set at "friends only" or "protected".
Do not accept friend requests from anyone you do not know in person.
Do not post private details such as home address, mobile or home telephone numbers or other personal details.
Never post photographs that have been taken in your bedroom
Never post photographs of others without their permission.
Never give out your mobile number.
If you get messages or images which upset you, do not reply. Keep a record and report them to a trusted adult or your network provider.
Think before you send messages or images – once you send them you cannot control them. Never pass on rude or embarrassing images or messages.
If someone makes you feel uncomfortable online – report it to a trusted, responsible adult and/or use the thinkuknow.co.uk website
Respect other people's privacy as well as your own.
Do not make someone else uncomfortable online.
Do not use a social networking site to bully another pupil including the editing and posting of inappropriate images, messages or comments or any aspects of cyberbullying.
Be aware of the legal consequences of your online activities.
You are not anonymous online, all correspondence can be sourced through the computer's IP address.

REMEMBER You can be traced online or on your mobile phone.

Be careful about what you say, what you upload, what you send, what you store.

Requests for further information in relation to ICT in the College should be addressed to:

Mr F. Cassidy

IT Manager
fcassidy664@c2kni.net

02890 205205