

North Coast Integrated College

Code of Practice for Acceptable Use of ICT/Internet –Students

North Coast Integrated college, in conjunction with C2K, has provided ICT resources for the use by students. They offer access to a vast amount of information for use in studies, acting like an enormous extension to the school library and offering great potential to support the curriculum.

The ICT resources are provided and maintained for the benefit of all students, who are encouraged to use and enjoy these resources, and ensure they remain available to all. Pupils are responsible for good behaviour when using ICT just as they are in a classroom or school corridor. Remember that **access is a privilege, not a right** and inappropriate use will result in that privilege being withdrawn.

Equipment

- Do not install, attempt to install or store programs of any type on the computers without permission.
- Do not damage, disable, or otherwise harm the operation of computers, or intentionally waste resources.
- Do not use computers for unauthorized commercial purposes, e.g., buying and selling goods.
- Do not open files brought in on removable media (such as CDs, memory sticks etc.) until they have been checked with antivirus software, and been found to be clean of viruses.
- Do not connect mobile equipment to the network (e.g. laptops, tablets, PCs, PDAs etc.) until they have been checked with antivirus software, and found to be clean of viruses.
- Do not eat or drink near computer equipment.

Security and Privacy

- Do not disclose your password to others, or use passwords intended for the use of others.
- Never tell any one you meet on the internet your home address, your telephone number, your school's name, or send them your picture, unless you are given permission to do so.
- Do not use the computer in a way that harasses harms, offends or insults other.
- Respect, and do not attempt to bypass, security in place on the computers, or attempt to alter the settings.

Internet

- Do not access the internet unless for study or for school authorized / supervised activities.
- Do not use the internet to obtain, download, send, print, display or otherwise transmit or gain access to materials which are unlawful, obscene or abusive.
- Respect the work and ownership rights of people outside the school, as well as other students or staff. This includes adhering to copyright laws.
- Do not engage in 'chat' activities over the internet.

Email

- Be polite and appreciate that other users might have different views from your own. The use of strong language, swearing or aggressive behaviour is not allowed.
- Never open attachments to emails unless they come from someone you already know and trust.
- The sending or receiving of emails containing material likely to be unsuitable for children or schools is strictly forbidden. This applies to any materials of a violent, dangerous, racist, or inappropriate content. Always report such messages to member of staff.

Monitoring

- Authorised ICT staff may inspect any ICT equipment owned or leased by the School at any time without prior notice
- All monitoring, surveillance or investigative activities are conducted by ICT authorised staff and comply with the
- Data Protection Act of 1998, the Human Rights Act 1998, the Regulation of Investigatory Powers Act 2000 (RIPA) and the Lawful Business Practice Regulations 2000.
- The school uses Securus the C2K online monitoring system to monitor content searched or used on all

computers in school.

Breaches

- A breach or suspected breach of policy by a school employee or pupil may result in the temporary or permanent withdrawal of school ICT hardware, software or services from the offending individual.

Please read this document carefully. Only once it has been signed and returned will access to the Internet be permitted. If any student violates these provisions, access to the Internet will be denied and the student will be subject to disciplinary action. Additional action may be taken by the school in line with existing policy regarding school behaviour. For serious violations, suspension or expulsion may be imposed. Where appropriate, police may be involved or other legal action taken.

Pupil's Internet Code of Practice

- I will only use the Internet when supervised by a teacher or adult.
- I will never tell anyone I meet on the Internet my home address, my telephone number or my school's name, nor will I arrange to meet them in person unless my teacher specifically gives me permission.
- I will never send anyone my picture without permission from my teacher / parent / carer.
- I will never give my password to anyone and I will log off when I have finished using the computer.
- I will not visit social networking sites or chat rooms and I will never respond to unpleasant, suggestive or bullying e-mails or bulletin boards. I will always report these incidents to a teacher or parent.
- I will not take part in cyber bullying. I will not use social networking sites, email accounts or my mobile phone to cause pain or inflict distress on others and I will make teachers aware of any incidents involving cyber bullying.
- I will not look for inappropriate material or distasteful images while on line and will report such things to a teacher or parent if I come across them accidentally.
- I know that my teacher and C2K will monitor the sites that I have visited.
- I understand that I can only access sites and materials relevant to my work in school and that I will not be able to use the Internet if I deliberately look at unsuitable material.
- I understand that I will not be able to use the Internet if I deliberately hack into schools or other systems.
- I know that the content of my e-mail messages will be monitored by the Network Manager.
- I will not download software from the Internet (including screen savers, games, video clips, audio clips, exe files) unless I have permission from my teacher.
- I will not use e-mail to send or encourage material which is pornographic, illegal, offensive or annoying or invades another person's privacy.

- I will respect the work of pupils, teachers. Online authors and online contributors and comply with copyright legislation.

Pupil's Name.....Class.....

I have read the Pupils' Code of Practice and I have discussed it with my child. We agree to support the school's policy on the use of the internet and are aware that offences will be dealt with according to the school's discipline policy, child protection procedures and , if necessary, the Police.

Signed (Parent / Guardian)Date.....

Additional Information for Parents

- A home computer with Internet access should be situated in a location where parents can monitor access to the Internet.
- Parents should discuss with their children the school rules for using the internet and implement these at home. Parents and children should decide together when, how long and what comprises appropriate use;
- Parents should get to know the sites their children visit, and talk to them about what they are learning.
- Parents should consider using appropriate Internet filtering software for blocking access to unsavoury materials. Further information is available from Parents Information Network (address below);
- Parents should ensure that they give their agreement before their children give out personal identifying information in any electronic communication on the Internet, such as a picture, an address, a phone number, the school name, or financial information such as credit card or bank details. In this way they can protect their children (and themselves) from unwanted or unacceptable overtures from strangers, from unplanned expenditure and from fraud
- Parents should encourage their children not to respond to any unwelcome, unpleasant or abusive messages, and to tell them if they receive any such messages or images. If the message comes from the Internet service connection provided by the school or C2K, they should immediately inform the school.

Further free advice for parents is available from the following sources:

<https://www.saferinternet.org.uk/advice-centre/parents-and-carers>

<https://www.nspcc.org.uk/preventing-abuse/keeping-children-safe/online-safety/>

<https://www.nidirect.gov.uk/information-and-services/your-childs-health-and-safety/internet-safety>