Computer and Telephone Systems: Acceptable Usage Policy

1) Introduction

a) The school expects its computer and telephone systems to be used in a professional manner at all times. The school provides these facilities at its expense for its own business purposes. It is the responsibility of each individual to ensure that these facilities are used for proper business purposes and in a manner that does not compromise the school, its employees, students, or partners in any way.

b) The school considers this policy to be extremely important. Employees and students found in breach of the policy may be disciplined in accordance with the school's disciplinary procedure. In certain circumstances, breach of this policy may be considered gross misconduct resulting in summary dismissal or expulsion. This policy document is to be read in conjunction with the school's disciplinary procedure.

2) Scope

a) The rules and guidelines set out in this policy apply equally to all employees and students of Cardinal Hume School.

b) The policy also applies to all third party suppliers and contractors granted access to the school's systems.

c) Compliance with the policy is mandatory.

3) General Rules on the Use of IT Systems and Telephones

a) IT systems, telephones, facsimile machines and any other system operated from time to time by the school, such as text messaging and instant messaging, must not be put to certain uses. Examples of inappropriate and/or wholly unacceptable uses are given below and are not limited to:

   i) Accessing or distributing material that could give rise to civil or criminal action against the school or bring the school into disrepute such as:

   1) Sexually explicit messages, images, videos, cartoons or jokes;
   2) Profanity, slander, or libel;
   3) Ethnic, religious, or racial slurs (including images, jokes, etc);
   4) Political, terrorist or propaganda material;
   5) Any other material that could be construed as harassment or disparagement of others based on their sex, race, sexual orientation, age, national origin, disability or religious or political beliefs;
   6) Drugs or criminal skills

   ii) Gambling (either on-line or via the telephone or facsimile);

   iii) Threatening, harassing, proposition or causing distress, annoyance, needless anxiety or discomfort to any other person or entity;

   iv) Circulating comments about employees, students, or other partners of the school which are abusing, objectionable, or otherwise inappropriate;

   v) Non-business use of the IT systems, telephones, or facsimile machines for unreasonable periods of time (including outside normal business hours). Improper use can lead to a waste of resources including time and may affect the efficient working of the school's network and systems;

Computer and Telephone Systems: Acceptable Usage Policy

vi) Sending offensive, demeaning or disruptive messages. This includes, but is not limited to, messages inconsistent with school's equal opportunities and harassment policies. You should not place on the system any message which you regard as personal, potentially offensive of frivolous to you or to any recipient;

vii) Entering into contractual commitments with external organizations without express authorisation to do so;

viii) Transmitting any sensitive data such as school or third party credit card details, passwords or customer account details;

ix) Using the school's IT systems or telephones for matters relating to a business that is not a client or supplier of the school and/or is not related to the provision of a service to the school, for example a personally owned business with no connection to Cardinal Hume School;

x) Downloading, copying or transmitting to third party the works of others without their permission as this may infringe copyright. You must comply with the terms of any licences to use copyright material. Publishing material on the internet does not mean that it is available for anyone to copy. You should assume that the content is subject to copyright unless the owner of that copyright states that you may download, copy or transmit the work.

b) Equipment that does not belong to the school must not be connected the school's network or systems without the express permission of the school's IT department, since such actions could compromise security, reliability and integrity of the school's IT systems. Examples include, but are not limited to, mobile telephones, personal digital assistants (PDAs), personal music players (e.g. iPods, MP3 players), storage devices (e.g. USB keys, portable disk drives, CD/DVD drives), local area networks (e.g. Wi-Fi or other school's networks), PCs and printers.

c) Employees and students shall keep Cardinal Hume Catholic School indemnified and held harmless from and against all actions, proceedings, claims, demands, cost, expenses, losses and damages whatsoever arising out of or in connection with the personal use by the employee or student of Cardinal Hume School's IT, telephone and other communication facilities.

4) Monitoring

a) The school reserves the right to monitor and record logging and traffic information on internet, e-mail, telephone usage, etc as well as actual content in the case of all business use e-mail and internet activity. The school also reserves the right to monitor and record logging and traffic information as well as actual content of all non-business use e-mails in the school's legitimate business interests at any time without notice. For example in the prevention and detection of crime, investigating or detecting unauthorised use, checking for viruses or other threats to the system, for record keeping purposes and checking compliance with regulations.

b) The school's failure to monitor in particular situations is not a waiver of the school's right to monitor in any or all situations.

c) Personal monitoring in relation to the school's IT systems and telephones.

d) Additionally, most organisations have a gateway between their e-mail system and the internet. E-mails will be subject to additional screening.

e) The school may disclose information to the Police in order to prevent or detect crime.

5) Confidentiality

a) You should not communicate anything in an e-mail, facsimile, or telephone message that you would not be comfortable writing in a letter or memorandum. All e-mail messages are

recorded in logs and back-ups. This means that even though a message may have been deleted from an employee or student's in-box, it may still be retrievable using other methods. You should note that electronic messages are admissible as evidence in legal proceedings.

b) You should never assume that internal messages are necessarily private and confidential, even if marked as such. Matters of a sensitive or personal nature should not be transmitted by e-mail unless absolutely unavoidable.

c) E-mail messages sent via the internet should be treated as non-confidential. Anything sent through the internet passes through a number of different computer systems all with different levels of security. The confidentiality of messages may be compromised at any point along the way unless messages are encrypted.

6) User accounts and passwords

a) Every employee and student is assigned a unique user account within the system. You must not use another's account.

b) You must not exceed or try to exceed the authorisation level provided by your account.

c) Employees must not impersonate anyone else's identity on the internet, telephone or on any Cardinal Hume School system. In all instances an employee's name, e-mail address and related contact information must reflect the actual originator of a message or posting.

d) You must not allow anyone else to use your password except authorised members of the IT department who may require access from time to time to provide support. If you anticipate that someone may need access to your confidential files in your absence you should arrange for the files to be copied to somewhere where that person can access them.

e) It is your responsibility to keep all passwords confidential.

f) To minimise security risks, the following rules should be applied when choosing passwords. These rules are based on recognised best practice and have already been adopted by thousands or organisations throughout the world. These rules are as follows:

 i Passwords must be at least six characters long;

 ii Passwords must contain characters from at least three of the following four clauses:

   1) Upper case letters (i.e. A, B, C, … Z)
   2) Lower case letters (i.e. a, b, c, … z)
   3) Numbers (i.e. 0, 1, 2, … 9)
   4) Non-alphanumeric (special characters such as punctuation symbols);

 iii) Passwords must not contain your username or any part of your full name;

 iv) Passwords cannot be the same as any that you have used previously.

g) These rules may appear daunting, but passwords using a number of elements can often be more memorable – the important thing is to choose something that is easy for you to remember and difficult for someone else to guess.

The following examples illustrate how the rules can be applied to produce memorable passwords, although these particular examples should not be used:

 i) Pa55word – uppercase 'P' and substitution of the number '5' for 's'
 ii) C0mput3r – uppercase 'C' and a mix of numbers and lowercase letters
 iii) Toon-army – uppercase 'T' and the inclusion of the '-' symbol

Computer and Telephone Systems: Acceptable Usage Policy

h) It is vital that passwords are not written down, since the biggest security breaches often come from within an organisation's own offices. If at any time you believe that someone may have discovered your password, please contact the support department.

i) Passwords expire every 60 days. A warning will be issued for 14 days before the account will be locked. The password should be changed at your earliest convenience to avoid the risk of being locked out of your account.

7) Internet usage

a) Any connection between the school's network and the internet presents the opportunity for third parties to attempt to access the school's network and the information contained therein. It is therefore extremely important that employees and students recognise that all use will be controlled and monitored to protect the school.

b) In addition to security issues, it is important that employees and students use the internet to increase their productivity rather than for non-business purposes. One consequence of use of the school's network for non-business purposes is that the responsiveness of critical business systems may be adversely affected.

c) You can use the internet for personal, non-business reasons out-with working/tutorial hours (e.g. before 8:45am, and after 3:45pm, and during a lunch break) providing that this does not interfere with the performance of your duties, consume significant resources or interfere with the activities of others. Please note that overtime payments cannot be claimed for time spent internet browsing for non-business purposes outside working hours.

d) Some internet sites are restricted via content filtering. This is to prevent access to unsuitable sites from the school's network. In order to prevent the risk of breaches of security, or adverse effects on the school's network, connections to the internet from the school's network will only be permitted in line with this policy.

e) Employees and students should note that the forwarding or storing material that is in breach of the policy may be the subject of disciplinary action. If you receive such material, you are advised to delete it immediately and contact the school's IT Department.

f) In addition to clause 3 of the policy, other uses to which the internet must not be put include, but are not limited to the following:

   i) Downloading, installing or running software or media files (including pictures, games, music, videos, screensavers, wallpapers, etc) or any PC either owned by the school of attached to the school's network. This includes software for business use since all software must be approved and tested by the school's IT department;

   ii) Posting information to public discussion groups ("newsgroups"), chat rooms, or other public forums on the internet on behalf of the school unless authorised to do so in advance by your line manager or tutor;

   iii) Establishing any unauthorised web pages, bulletin boards, or other mechanism that provides public access to information about the school;

   iv) Establishing Electronic Data Interchange (EDI) or other electronic business system arrangement.

If you are unclear as to whether your internet usage is unacceptable or excessive, please discuss this with your line manager or tutor. (If unsure take advice from Network Manager)

Computer and Telephone Systems: Acceptable Usage Policy

8) E-mail usage

a) E-mail is an effective method of communication provided primarily for business use. Occasional non-business use is permitted, but only in line with the policy. Non-business use of e-mail must not interfere with the performance of your duties, consume significant resources of interfere with the activities of others.

b) Employees MUST ensure to encrypt any emails that may contain sensitive/personal/confidential information. This is the responsibility of the individual and failure to comply would be breach of Data Protection Act and will be dealt accordingly. To encrypt an email you must write the word "**Confidential**" in the subject line of your email before sending.

c) Employees should note that the forwarding or storing of material that is in breach of the policy is likely to be the subject of disciplinary action. If you receive such material, you are advised to delete it immediately and contact your line manager or tutor who will seek advice if necessary.

d) You must not transmit chain letters, junk e-mail or spam (unsolicited messages). You should be aware that the internet is the source of a large number of hoaxes alleging security problems such as viruses that erase hard drives for example. Any alerts or similar warnings should be forwarded to the school's IT support department and no further action taken unless advised otherwise.

e) If you receive e-mail that contains material that is offensive or inappropriate to the school environment that you must delete it immediately. Under no circumstance should such mail be forwarded either internally or externally.

If you would not say it in public, or send it by post the DO NOT e-mail it.

9) Legality

a) You should ensure that the transmission of "personal data", for example databases, spreadsheets, outside the school does not infringe the principles of the Data Protection Act (DPA). A spreadsheet containing information such as a person's name, age, address, etc is covered by the DPA. "Personal Data" is information recorded on a computer or relevant filing system (or recorded with intention that it will go into either), which is biographical, focused and affects privacy. If you have any doubts regarding the transmission of personal data, please contact [the Network Manager].

b) Any information, software or graphics from any published format (books, magazines, brochures and the internet) are likely to be protected by copyright law, regardless of whether a copyright notice appears on the work. Any breach of copyright will be taken very seriously.

c) Although you should be diligent in housekeeping your e-mails, recipients may keep a record that is discoverable in the future. You must therefore treat all e-mails sent internally and externally as a permanent record. Further, copy e-mail transmissions may be disclosed in litigation. Before you send an e-mail, think carefully about its content and ask yourself how you would feel if you received that message or knew it may be disclosed in court. Your e-mails can be "discovered" in future by outside parties if relevant to litigation.

10) E-mail filtering

a) E-mail content filters protect the school from computer viruses and other malicious software designed to damage systems or to steal information. It is important that unsolicited messages do not overload the e-mail system with unwanted messages – examples of these include advertisements, automated mail-shots (sometimes called spam), chain mail, known hoaxes and scams.

b) The content filter is also used to support the school's policy and guidelines. Once the content filter has blocked an e-mail, it is placed in a "quarantine" queue.

c) The quarantine queue is checked on an hourly basis between 08:00 and 18:00 on business days and any business related e-mail will be forwarded without it having to be requested. However, if a business related e-mail has been quarantined and you need it more urgently then you can forward the notification to the IT Helpdesk to request its immediate release.

d) For more information about e-mail filtering please refer to the practical guide, which is available on the school's intranet.

11) Telephone usage

a) The school's telephone system and mobile telephones are meant for school purposes only and usage is kept in line with the policy. Inappropriate and unacceptable use of the telephone system is outlines in clause 3 of the policy.

b) Our aim is to provide a swift and professional service to all our business clients, partners and internal callers. This aim is adversely affected when outgoing and incoming personal calls prevent genuine business calls getting through either directly or via the switchboard.

c) Utilisation of the school's telephone system for personal use should be kept to an absolute minimum.

d) If you need to make or receive a telephone call in an emergency, the school will permit the use of its telephone network at any time.

If you are ever unclear as to whether your telephone usage is unacceptable or excessive, please discuss this with your line manager or tutor.