SHIMNA INTEGRATED COLLEGE

INTERNET AND E-MAIL USAGE POLICY

Introduction

1. This document sets out the policy of SHIMNA INTEGRATED COLLEGE (herein after known as Shimna), in relation to the use of Internet and e-mail facilities within the college. The policy applies to all staff, students and visitors who have been given permission to use Shimna resources to access Internet or e-mail facilities. The policy is available as hardcopy from the college and is also available to read or download from the college web site www.shimnacollege.org.uk

2. Individuals using non-Shimna equipment or facilities for official business must ensure that such use does not compromise the security of official data or expose Shimna systems or equipment to risk of disruption from any source, such as a virus attack or unauthorised access. Staff should seek advice, as necessary, about IT security matters via their usual departmental IT contacts.

3. Internet and e-mail facilities can deliver significant business benefits and advantages when used appropriately and responsibly. However, careless or negligent use may waste resources and cause financial loss and damage to reputation. For example, unnecessary and/or unauthorised Internet/e-mail usage may cause network and server congestion, slow service delivery, reduce efficiency, consume supplies, and tie up shared resources. Also, misuse may lead to complaints or legal proceedings against Shimna or individual members of staff.

4. The policy is intended to protect the interests of Shimna, as well as the interests of users, and **to ensure that individuals are not at risk of disciplinary action, criminal proceedings or civil action as a result of misunderstanding or lack of guidance.**

5. All staff who use, or intend to use, Shimna Internet or e-mail facilities for any purpose will be required to acknowledge that they have read, understood and will adhere to, the Shimna policy and any related departmental policies. Such undertakings will be renewed if the Internet and e-mail usage policies change. Failure to comply with the requirements of the Shimna policy, will result in disciplinary action – including dismissal.

Monitoring and Privacy

6. The Lawful Business Practice Regulations 2000 require employers to inform staff if there is a possibility that interceptions of communications might take place. Staff should note that, as is permitted by legislation, Shimna and C2k will monitor and review Internet and e-mail activity, analyse usage patterns and may publish resultant data:

(traffic monitoring 1). Shimna will also monitor the content of e-mails, files, sites visited etc. as and when this is considered necessary in order to ensure the integrity of Shimna systems and that users are complying with all relevant usage policies and guidance,

(content monitoring 2). Use will be routinely monitored from time to time, and may be specifically monitored at any time when this is deemed necessary for compliance or other reasons, including the prevention or detection of illegal activities.

7. Users of Shimna ICT resources, including Internet and e-mail facilities, should be aware, and must accept as a condition of use, that their usage of such facilities might be monitored and should have no expectation of privacy whether use is for the conduct of official business or for personal use.

1 ***traffic monitoring*** – recording and analysing websites visited, the addresses to which emails are sent, file transfers into and out of Shimna networks .etc. - the equivalent of recording the duration and destination of telephone calls.

2 ***content monitoring*** – looking at the actual content of e-mails, files etc. – the equivalent of recording and listening to the content of telephone calls.

8. Shimna reserves the right to inspect and examine any and all IT equipment (including personally owned equipment) used in Shimna, used for the conduct of official business, or connected in any way to the Shimna Network, in order to ensure compliance with Shimna Internet and e-mail usage policy. Therefore, users should clearly understand that if they bring into the workplace personal IT equipment of any nature, including laptop computers, mobile phones, camera phones, personal digital assistants (PDAs), portable media players, digital video equipment, webcams etc, or data storage devices such as floppy disks or CD ROMS, any such equipment or ancillaries, and data held thereon, may be inspected at any time to ensure that they do not pose a risk to Shimna whether by way of virus infection, hacking software or the presence of improper, offensive or illegal material.

Detailed Guidance

9. Detailed guidance is set out in the attached policy document entitled "Guidance on the Use of Shimna Internet and E-mail Facilities". All users must familiarise themselves with its contents and remember that the policy applies when using Shimna resources for any purpose and also when using non- Shimna resources (e.g. home computers/personal e-mail accounts) to conduct official business.

Consultation with Trade Union

10. The terms of this circular have been agreed with the Trade Union Side of the Joint Negotiating Council for Northern Ireland Education and Library Boards.

11. Any enquiries about the content or application of this circular should be addressed to the principal

June 2014

GUIDANCE ON THE USE OF SHIMNA INTERNET AND E-MAIL FACILITIES

Access to Facilities

1. Shimna may make Internet and e-mail facilities available to staff for use in carrying out official duties. The decision as to which staff (or others) should have access to Internet or e-mail facilities is at the discretion of Shimna. Departments and agencies may prevent connection of certain machines (holding sensitive data or applications) to the Internet or restrict use of Internet features such as file transfers, and will bar access to sites identified as containing inappropriate material. Shimna accepts and implements the "Acceptable Use Policy" required by C2K.

2. C2k are responsible for the issue of User IDs and/or passwords to maintain individual accountability for Internet and e-mail usage. Individuals will be held responsible for the security of IDs and passwords. C2k/Hewlett Packard also manages the web filtering and monitors web usage continually. A log is kept of websites visited by all users.

3. Shimna must ensure that facilities provided for e-mail and Internet access meet all relevant health and safety legislation.

4. Users must respect the privacy and legitimate rights of others, just as would be appropriate in any other work activity. **Individuals will be held accountable for any misuse or breach of security, including confidentiality. Such misuse may lead to disciplinary action**. Activities such as accessing, possession or dissemination of pornography or other offensive material, serious harassment or bullying, propagation of any virus or otherwise interfering with the integrity of Shimna systems, or the possession of hacking software on official premises, **are likely to result in dismissal. Where circumstances dictate, Shimna will inform and co-operate with relevant legal enforcement bodies.**

5. Access to Internet and e-mail facilities may be withdrawn at any time as a result of, or pending the outcome of, investigations into suspected misuse.

General Responsibilities of Users

6. All of the usual Shimna rules relating to conduct and normal standards of behaviour apply just as much when using Internet or e-mail facilities as at other times. Users must at all times conduct themselves responsibly and honestly when accessing the Internet or when using e-mail facilities. They must ensure that their actions do not:

a. waste time or resources;

b. expose the Shimna network, or data held thereon, to risk of corruption, loss or inadvertent disclosure;

c. cause offence to colleagues or others;

d. breach any law or statute; or

e. otherwise bring Shimna into disrepute.

7. Unacceptable behaviour - such as harassment, bullying, dissemination of inappropriate material, offensive remarks or comments of a racial or sectarian nature, or regarding sexual orientation - is just as serious an offence if made in the course of using IT facilities as at any other time, and will not be tolerated. Inappropriate material may include, but is not limited to, any material of a pornographic, sexist, racist, sectarian, violent or offensive nature, whether in pictures, cartoons, words, sounds or moving images, and whether or not purporting to be of a humorous nature.

8. **Users should note that they might be personally liable to prosecution, and open to claims for damages, should their actions be found to be in breach of the law**. In cases of harassment, a claim by a user that he/she had not intended to harass or cause offence will not in itself constitute an acceptable defence.

9. **Users should be aware that the possession of child pornography is a criminal offence.** Shimna will fully co-operate with law enforcement authorities to identify and take action against any member of Shimna accessing, possessing or disseminating such material. Individuals found to have been involved in any way in the possession or dissemination of child pornography using Shimna IT systems will face serious disciplinary action with a high probability of dismissal irrespective of whether or not they are prosecuted or convicted under
the criminal law.

What Users MAY Do

10. Within this overall context users may (subject to the safeguards and conditions set out in this and any other relevant policy or guidance):-

a. use e-mail to communicate with colleagues, customers, suppliers and other interested parties in carrying out their college duties;

b. use the Internet to research relevant and potentially relevant information sources in carrying out their duties. In doing so, users may glean relevant information from trusted third parties (including news sites), provided prior approval for such access has been granted by C2k; and

c. participate (subject to Shimna approval) in officially

sanctioned newsgroups or chat rooms in the course of business relevant to their duties. In any such use of Internet/e-mail facilities, users must identify themselves honestly, accurately and completely.

When participating in a chat forum or newsgroup users must:

a. refrain from any political advocacy and from the unauthorised endorsement or appearance of endorsement of any commercial product or service;

b. give due regard to maintaining the clarity, consistency and integrity of Shimna, and avoid making any inferences that may prove inappropriate from a Shimna perspective;

and must not:

a. reveal protectively marked information, student/staff data, or any other material covered by Shimna policies and procedures; and,

b. use Shimna Internet facilities or computing resources to violate laws and regulations applicable in Northern Ireland in any way or to compromise the security (including confidentiality) of Shimna data.

What Users MUST Do

11. At all times users must:-

a. keep all passwords or user IDs confidential - the sharing of user IDs or passwords is prohibited;

b. be alert to the risk of leaving an unattended machine logged on, which could lead to unauthorised use of their account and user ID;

c. follow the security procedures approved for use with their system to ensure that any file downloaded from the Internet is scanned for viruses before it is accessed or run. Users who download such files, or who open attachments to e-mails, are responsible for ensuring that they are subjected to appropriate anti-virus scans (checking with the ICT Manager as necessary);

d. report immediately any indication of virus or other attack;

e. report immediately to the ICT manager or, if appropriate, to the principal, the receipt of inappropriate or offensive material delivered via e-mail;

f. all users must comply with all relevant legislation on copyright, property theft, libel, fraud, discrimination and obscenity;and software licensing rules and download only software with direct college use and do so in accordance with Shimna policy;

g. as far as possible, schedule communication-intensive operations such as large file transfers, video downloads, mass e-mailings, etc. for off-peak times.

What Users <u>MUST NOT</u> Do

12. Users must not:-

a. arrange to auto-forward e-mails from their Shimna account to personal e-mail accounts, or from their personal e-mail account to Shimna accounts. E-mails received into a Shimna account may be forwarded once their contents have been vetted to ensure that the forwarding of the e-mails does not contravene guidance in respect of protectively marked material;

b. propagate any virus or program designed to infiltrate a system (without the user's knowledge) to gather information (e.g. worm, Trojan horse) or other type of malicious program code;

c use any Shimna facilities to disable or overload any computer system or network, or attempt to disable, defeat or circumvent firewalls or any Shimna ICT security facility intended to protect the privacy or security of systems, networks or users;

d. forward, send or store e-mails or other files containing inappropriate material;

e. knowingly connect to any Internet site that contains inappropriate material. When such a site is inadvertently accessed, users will immediately disconnect from the site, regardless of whether that site had been previously deemed acceptable by any screening or rating program. **<u>Such inadvertent connections must be reported immediately to the ICT Manager</u>** so that appropriate action to bar access to the site can be taken and to safeguard the individual in the event of any subsequent investigation;

f. use any Shimna systems or facilities to commit infractions such as harassment, unauthorised public speaking, misappropriation of intellectual property or misuse of Shimna assets or resources;

g. intentionally access, archive, store, distribute, edit, record, or reproduce (on screen, hardcopy or via audio) any kind of inappropriate material on any Shimna system;

h. use Shimna facilities to download and/or forward non-educational related software or data including music, graphics, videos, text, games, entertainment or pirated software;

i. use Shimna facilities to play internet games or forward chain letters (even in the user's own time);

j. use Shimna facilities to participate in chat rooms, forums or newsgroups unless this is for educational purposes and has been approved by management;

k. upload any software licensed to Shimna or data owned by Shimna without the express authorisation of the principal or ICT Manager responsible for the software or data;

l. transfer via the Internet (as opposed to the Shimna Intranet) files containing RESTRICTED Shimna data unless the data is first encrypted using a product approved by the C2k. Files containing RESTRICTED material may be transferred via Shimna Intranet. However, files containing Shimna data with a protective marking higher than RESTRICTED must NOT be transferred electronically.

m. remain connected to the Internet while not actively using the resource.

PERSONAL USE

Definition

13. Personal use is defined as any use of Internet or e-mail facilities that does not stem from a requirement directly relating to staff/students educational needs. Thus accessing a site for research purposes, for example searching social security policy or employment law developments, is official use only if such access is necessary as part of the users work. Accessing such data only out of personal interest, or to broaden general knowledge in that area, would be classed as personal use if the information is not actually required to discharge duties effectively.

14. Any access or use which is unrelated to official duties, for example, accessing general news sites, travel information, personal banking, sending or receiving personal e-mails and so on, would be classed as personal use.

Guidance on Personal Use

15. Shimna may permit staff to use Shimna facilities for personal use, in their own time, providing that such use does not compromise the security of official data, result in increased costs or delays or have any negative impact on the Shimna network or on the effective discharge of official business. Own time is when an individual is not on duty, such as before signing in or after signing out or during lunch or other officially sanctioned breaks. The facility is granted at the discretion of management and may be withdrawn at any time for operational reasons, or if misuse is suspected or detected.

16. Users are reminded that all Internet and e-mail use is subject to monitoring. Such monitoring does not differentiate between official and personal use. Users should therefore ensure that anyone who may send personal e-mails, or other material, to their official e-mail address is aware that the content of such emails may be monitored. Use of

Shimna facilities for personal use will be deemed as acceptance that usage, and on occasions, content, will be monitored.

17. Subject to Shimna policies in relation to personal use, users may in their own time:-

a. use Internet access for personal research, provided such use has been approved by local management;

b. use the Internet for the occasional purchase of goods and services, for example, books, flights, CDs, and so on, provided payment is made by the individual, and delivery of items purchased is to a private address. The user must not create any unauthorized contractual liability on the part of Shimna. Shimna does not accept any responsibility for the security of credit card details, or any other payment method used. Nor does Shimna accept any liability for financial loss, whether as a result of fraud or otherwise, suffered while using Shimna systems for personal transactions. All such use is entirely at the individual's own risk;

c. make occasional use of Shimna facilities for on-line banking. All such use will be at the individuals own risk - Shimna cannot accept any liability for losses or for any other liabilities arising out of such transactions, howsoever caused; and,

d. make occasional use of Shimna e-mail accounts set up on their behalf, to send, forward or receive personal emails – subject to the conditions for using e-mail facilities set out in this policy. Personal e-mails must be clearly marked as being "personal".
It is an explicit condition of using this facility that users accept that the content of such e-mails may be accessed, by management and/or IT staff, without notice or any requirement for further consent. While it is not intended to undertake routine monitoring of the contents of e-mails (personal or otherwise), e-mail traffic may be accessed at any time either as a result of checking an individuals e-mail account for business reasons if they are absent from work, or as part of an exercise to monitor compliance with internet and e-mail usage policy.

18. Users must not make excessive use of any of the above facilities to the detriment of their official duties.

Restrictions on Personal Use

19. Users must not:-

a. use Shimna Internet or e-mail facilities to carry out any activities for personal gain including, for example, share dealing or monitoring, investment portfolio management, or gambling; or

b. set up a personal e-mail account using departmental or agency resources unless prior approval to do so has been given by the principal

Teachers Responsibilities

20. It is the teachers' responsibility to ensure that students are aware of the correct usage of the internet in Shimna and the consequences of its misuse.

NOTE: Students in Year 8 are instructed on the many advantages the internet can offer. They are also made aware of the more sinister side and are told how to conduct themselves while online in Shimna and at home where they may be using chat rooms, MSN, bebo etc. The Year 8 teacher and ICT Manager have attended a CEOP training course and are qualified to discuss this information with the students. Students are continually made aware of safe internet usage throughout their time in Shimna.

Teachers should use their professional experience and common sense as to what restrictions and guidelines they wish to impose during their lessons. Teachers should be vigilant when students are using the internet and monitor the information they are accessing, taking appropriate action as and when needed.

The misuse of Shimna internet/email facilities can lead to a student being denied access to the internet for a specified period. Certain incidents as outlined on page 3-4 **(General Responsibilities of Users**) of this policy can lead to Law Enforcement Agencies being brought in and legal action being taken against an individual/s.

Copyright and Similar Issues

21. Shimna will, where it is deemed appropriate:-

a. retain the copyright to any Shimna material posted to any forum, newsgroup, chat room or World Wide Web page by users in the course of their duties; and,

b. assume ownership of any legitimate software or files downloaded via the Internet on to Shimna networks. Any such files or software may be used only in ways that are consistent with their related licenses and/or copyrights.

POLICY ON THE USE OF MOBILE PHONES, TEXTING, COMPUTERS AND THE INTERNET

Introduction

The college is very aware of the educational benefits and advantages the good and proper use of modern communications' technology; it is also very aware of the personal hurt, harm and damage that can come to individuals through the misuse and abuse of this technology. Consequently, the college is concerned to make the best possible provision for the safe use of communications' technology and for the well being of both the students and the members of staff who, in turn, are responsible for adhering to and /or implementing this policy.

1. Students' Use of Mobile Phones and Texting

- Although students may bring mobile phones to college, they may not use them during class. If they are caught using their phones during teaching time, they will be taken from them and kept in the college for collection by a parent or guardian.

- Photographs / videos of students should not be taken using a mobile phone (or by any other means) without their prior consent.

- The sending of offensive text messages, bullying by text and the taking and sending of inappropriate mobile photographs will be treated as a serious offence that may lead to suspension. Should the college decide that the offence is sufficiently serious, the Police will be informed.

2. Mobile Phone Contact with Students by Members of Staff

Members of staff need to be aware of the opportunities for abuse through the misuse of mobile phones and text messaging. While the proper use of such media can be beneficial, they must be vigilant and alert to the possibilities of misuse and the consequent harm to students. Staff members must also be vigilant to protect themselves, consequently, they should **NEVER** give their mobile phone numbers to students.

Members of staff should adhere to the following guidelines:

- Most members of staff will not be required to phone or text young people. Consequently, they should not have a student's mobile phone number on their phone.

- They should contact a student via mobile phone only when absolutely necessary. Where possible, they should use the college phone to contact students.

- Parents' permission should be sought if a member of staff is likely to be contacting the young person via mobile phone.

- If a member of staff has a student's phone number, it should only be used for the purposes it has been given for eg communicating matters concerning the college, course work etc. It should **NEVER** be used for social or informal communication with the student.

3. Staff Texting to Students

- Members of staff should only text students in an emergency situation.

- Texting, if necessary, should be for communication and not conversation or social interaction.

- Members of staff should **NEVER** respond to informal, social texts from students.

- Texts should only be used for the purposes of, for example, communicating information re: for example, the times of exams, sports team information etc.

- If texting turns into a "conversation", communication should be ended. The texting of a message or information that could be misconstrued, or misinterpreted, should be avoided.

4. The Use of College Computers

- Members of staff are required to adhere to and implement the college's comprehensive Internet Policy. They will monitor carefully the student's use of college computers to ensure that they are not sending offensive e-mails, or logging on to adult or other inappropriate chat rooms and web sites. The abuse of the use of computer by students will be treated as a serious offence that may lead to suspension. Should the college decide that an offence is sufficiently serious, the Police will be informed.

- Members of staff should only divulge their home email address when it is essential for a student/s to know it in pursuit of their college work eg sending and receiving course work.

5. Use of the Internet

In addition to the requirements of the college's Internet Policy, members of staff should adhere to the following:

a. Social Networking Sites and Chat Rooms

- Members of staff should avoid communicating with students via social networking sites and chat rooms.
- If a member of staff is concerned about a student, or if a student discloses something to them via a social networking site or a chat room, the disclosure must be treated in the normal fashion.

b. Websites

- Members of staff should make it very clear to students that websites should not be used to make arrangements to meet up with each other casually. They need to be reminded that they don't know who is reading their conversation.

- Members of staff should be aware that by advertising dates and times of events online, there is the possibility other people, who would not have otherwise heard of events, may turn up without warning. As this will probably not be welcome, members of staff

should think carefully about what events they want advertised on websites, and what they would do if this situation arose.

In the case of an alleged misuse and abuse of the above means of communication by a staff, the allegation will be treated seriously and will be dealt with via the college's disciplinary procedures; any such case may involve the Police.

6. Conclusion

The college will do all that it can to keep abreast of the continuing developments in communications' technology, and to inform students and staff about its proper use, as well as the possible outcomes of its misuse and abuse by students and staff.

The college will expect strong parental support and co-operation when dealing with the misuse or abusive use of mobile phones and the college's computer and Internet systems by students.

The Board of Governors agrees with, and fully supports the contents and implementation of this policy.

June 2014