



Hazelwood Schools

Security Policy

Review 2011

1. Scope

1.1 The Policy covers:

The deployment and use of Hazelwood Schools electronic information systems (i.e. all computers, peripheral equipment, software and data) within and between Hazelwood Schools property, or belonging to Hazelwood Schools but located elsewhere;

The use of information systems not owned by Hazelwood Schools and located outside of its property, where such use is effected from or via equipment located on Hazelwood Schools property, or by equipment belonging to Hazelwood Schools.

All use of Hazelwood Schools' computer network;

The security of hardware, software and data; the security of personnel using information systems; and the security of Hazelwood Schools' assets that may be placed at risk by misuse of information systems.

1.2 In respect of copyright and data protection aspects, the Policy covers the use of information systems not owned by Hazelwood Schools or located on its property, but used by Hazelwood Schools staff for business purposes connected with Hazelwood Schools.

2. Objectives

2.1 Hazelwood Schools seek to protect its assets from loss and to provide a secure working environment for its staff. The objectives of the Policy are to ensure as far as is reasonably possible that

Hazelwood Schools' assets are secure against loss by theft, fraud, malicious or accidental damage, or breach of privacy or confidence, and

Hazelwood Schools is protected from damage or liability resulting

from use of its facilities for purposes contrary to the law of the land.

3. Legislation and Other Policy

The Policy is to be read in the context of the following legislation:

- .Data Protection Act (1998)
- .Computer Misuse Act (1990)
- .and any other relevant legislation.

4. Application of the Policy

Enforcement

It is the specific responsibility of the Senior Management team to ensure that the Policy is carried out. All staff have a personal responsibility to ensure that they, and others who may be responsible to them, are aware of and comply with the Policy.

Breach

It is the duty of the Senior Management team to take appropriate action to prevent breaches of the policy. Where such action is outside of the remit of Senior Management team they will notify the appropriate IT Support department.

Review and Audit

The Security officer is responsible for regular review of the Policy in the light of changing circumstances. Hazelwood Schools Internal Audit Department has a brief to ensure that the Policy is appropriate for the protection of Hazelwood Schools' interests.

5. Acceptable Use

Acceptable use is defined as use for the purposes of:

- Teaching and learning
- Research
- Personal educational development

Administration and management of Hazelwood Schools business

Development work and communication associated with the above

Consultancy work contracted to Hazelwood Schools

Use of computer facilities for limited personal correspondence, where not connected with any commercial activity, is at present regarded as acceptable.

The Rules for Use of Electronic Information Systems which form part of Hazelwood Schools, are binding on all staff and will form part of the contract of employment. The Rules will be regularly reviewed by the Senior Management team for adequacy.

It is Hazelwood Schools policy that there will be a Code of Good Conduct which will be reviewed regularly by the Senior Management team and circulated to all members of Hazelwood Schools. Users are expected to abide by the Code.

It is Hazelwood Schools policy that all use of the facilities shall be lawful, honest and decent, and shall have regard to the rights and sensitivities of other people. Users are expected to comply with the Computer Misuse Act 1990 which makes hacking and the introduction of viruses a criminal offence and the Criminal Justice Act 1994 amended to the Obscene Publications Act under which it is a criminal offence to create, store, download or transmit obscene material. This includes storage of files sent to users as e-mail attachments

The Security Officer has responsibility to take all reasonable steps to stop unacceptable use of information systems. If the Security Officer is unable to carry out the duty required, the responsibility will fall to the Senior Management team. The team will be guided on policy issues by the Local Authority Data Protection Officer, Security Officer and any appropriate bodies.

6. Enrolment

Where the job requires access to Hazelwood Schools' information systems a user will be enrolled viz:

NT

A unique user name and initial password will be allocated to each new user. If access to specific systems is required, this will be carried out upon the initial signed request from the agreed authorisers. Passwords expire on a regular basis. It is the user's responsibility to create their own password, within the guidelines set out below.

Amendment of an existing user's access will be actioned upon receipt of the signed request from the agreed system authorisers.

Internet

The same unique user name, but a different password, will be allocated to each new user upon the signed request from the authoriser with the appropriate business justification. Passwords DO NOT expire, and are not alterable by the user

The use of information systems and networks shall be restricted to enrolled users.

Passwords

Where the relevant information system allows the user to create and maintain their own passwords, the password must fall within the following guidelines.

Length a minimum of 8 characters, a maximum of 10 characters

Composition any alpha-numeric character, but it must begin with a letter

Repetition no password can be repeated within 6 months

Uniqueness the same password may be used for each system, although for good security practice it is best that they are different

7 Clear Desk Policy

All staff are responsible for the security of information in their control. During absences from the work place, staff must ensure that information is secured appropriately. This is known as the clear desk policy. At the close of business each day, staff should take precautions to ensure that information, especially security classified information is protected from

unauthorised access. The following should be observed by all staff as part of an effective lockup procedure:

8 Filing

Security classified information should not be circulated uncovered or loose. Information that can be filed should be placed on an appropriate file as soon as possible after its creation or receipt. This is usually after registration. If used correctly, the records management system and tools should also readily identify the location of files.

9 Procedure for the disposal of classified information: Paper based resources

The disposal of unwanted information is a process that requires careful consideration from a security and records management perspective. The schools' Senior Management team may only destroy surplus copies of classified information. All other destruction must be authorised by the Records Manager.

Information of any description is not to be disposed of in waste paper baskets or general refuse bins.

10. Physical Security

Equipment will be secured against theft and damage to a level that is cost-effective.

It is the responsibility of the computer user to attend to the following:

- Taking appropriate security precautions in respect of computers under his/her control.

- Observing good practice recommendations for security in respect of facilities provided on multi-access computers and networks.

Damage to equipment, software or data resulting from failure to observe this policy is deemed to be the responsibility of the defaulter.

Control of access to personal data is the remit of Hazelwood Schools Data Protection Officer, who will ensure that information about rights

and responsibilities under the Data Protection Acts (1998) is made available.

11. Monitoring

The Security Officer, or System Administrator as appropriate, is responsible for ensuring that usage of resources will be logged in sufficient detail to identify defaulters where technically possible.

The Security Officer, or System Administrator, as appropriate, will monitor and police the use of computer facilities. Monitoring data will be collected only to assist investigation of a suspected security breach or other misuse.

Security support staff shall not monitor personal information except in specific instances where a suspected breach of security or other substantive offence requires it. Every such incident will be reported to Hazelwood Schools head teacher, where the suspected offender is a situated. Details of the incident will be logged promptly in a central record which will made available for inspection by the head teacher.

The Security Officer is empowered to authorise a software audit of Hazelwood Schools' equipment, where it is deemed necessary.

12. Duties of System Administrators

System administrators have responsibility for maintaining the integrity of computer systems and data held on them, and for ensuring the systems are not misused.

System administrators are provided with privileged access to computer systems in order to carry out their responsibilities. They have a duty to use such privilege at all times in a professional manner and within the interest of Hazelwood Schools.

The Security Officer is responsible for ensuring that the duties of system administrators are carried out.

Code of Good Conduct and Practice

Hazelwood Schools has a set of Rules and a security policy governing the use of electronic information systems. In addition, Hazelwood Schools' Information Systems has issued the following Code of Good Conduct and Practice. These guidelines do not constitute a set of rules, but are an indication of expected behaviour and good practice when using the computing facilities.

1. What you may use Hazelwood Schools Computer Equipment for

Computers are provided for the purposes or for Hazelwood Schools business. There is no objection to your making reasonable use for personal purposes such as electronic mail, providing you observe the following code.

Don't waste materials, or waste time on the computers to the detriment of your job.

Don't send offensive, or unsolicited junk, or nuisance mail. Also remember mail might accidentally reach somebody for whom it was not intended.

Your use must be lawful, honest and decent, and must have regard to the rights and sensitivities of other people. This means that any use that is obscene or with the intent of annoying or offending somebody else is forbidden.

The law requires that you don't hold any information in electronic form about living persons unless you are registered to do so.

2. Respect Computer Equipment

Please treat computer equipment with respect - it is there for your benefit.

No eating or drinking around the computer equipment.

Don't load any files from removable discs on Hazelwood Schools' PCs unless you have had them virus checked

beforehand. The security precautions in place will not permit the installation of program .exe files

Don't delete, disable or tamper with any software or settings provided by Hazelwood Schools.

Don't tamper with the hardware or any network or power connections.

Don't move the equipment.

3. Using the Network

Never attempt to gain access to another person's account (username) on any computer. If you do you are breaking the law.

4. Look After Your Usernames and Passwords

When you are enrolled you will receive a username and password.

It's your responsibility to keep your username secure. Never allow anyone else access to it.

Keep your password secret; Try to avoid using your name, your partner's name, your car registration or anything else that someone might guess. If you have to write it down, disguise it. If you think someone might have watched you typing it in advise Technical Support immediately.

It's safer to use a different password for every computer system allocated to you.

Don't leave a logged-in session unattended, even for a moment.

Make sure you log out when you finish using the computer.

Never use anyone else's account, with or without their permission.

5. Look After Your Equipment

It's your responsibility to keep equipment under your control free from viruses or anything else with the potential of causing damage.

6. Look After Your Data

You, not Hazelwood Schools, are ultimately responsible for the security of the data. If you hold important data on a PC, you should ensure it is on the correct drive for Hazelwood Schools' back-up procedures.

Power, disc and system failures usually take effect without warning. Think about the consequences before you use the computers. The following is good practice and is recommended.

- Save your files at frequent intervals

- Read the messages displayed at log-in; this facility is intended to warn you of any imminent service interruptions.

It is sometimes possible to retrieve files that have been deleted accidentally, but you shouldn't rely on this feature. A charge may be levied in respect of procedures used in retrieving files.

If you leave Hazelwood Schools your usernames will be deleted.

7. Observe Copyright Restrictions

Don't copy any data without permission. This includes copying text or graphics - whether by using a scanner or by typing it in.

8. Rules and Discipline

You are bound by Hazelwood Schools' Rules for Use of Electronic Information Systems. You will have received a resume when you joined Hazelwood Schools in your Employee Handbook. You should ensure you are familiar with these Rules.

The Security Policy for Electronic Information Systems is also available from the head teacher

If you break the Rules:

Your permission to use Hazelwood Schools computers may be withdrawn.

You are also liable to disciplinary action under Hazelwood Schools procedures.

If you believe you have been treated unfairly you have the right of appeal.

RULES FOR USE OF ELECTRONIC INFORMATION SYSTEMS

Electronic information systems of Hazelwood Schools may be used only by the staff of Hazelwood Schools and other persons authorised in writing by the Director of Information Systems

The information systems are used on the understanding that Hazelwood Schools will not accept any liability whatsoever for loss, damage, or expense which may result from the computing facilities, except to the extent that such loss, damage, injury or expense are attributed to negligence or breach of statutory duty on the part of Hazelwood Schools or any of its servants or agents acting in their capacity as such.

Username and other allocated resources shall be used only by the registered holder. Users shall maintain a secure password to control access to their usernames on all systems. Sharing of usernames will not be permitted save in exceptional circumstances by prior written agreement of a member of the Senior Management team.

No person shall by any wilful or deliberate act or by failure to act with due and reasonable care jeopardise the integrity of the computing equipment, its operating systems, systems programs or other stored information, or the work of other users, whether within Hazelwood Schools or in other computing locations to which the facilities at Hazelwood Schools allow connection.

Unauthorised access to computer material (i.e. a program or data) and unauthorised modification of computer material are forbidden by law (Computer Misuse Act 1990) and by these Rules, which endorse the Guidance on the Computer Misuse Act.

Computer facilities available for use within Hazelwood Schools may be used only for:

- o Teaching and learning
- o Personal development program
- o Administration and management of Hazelwood Schools business
- o Development work and communication associated with the above

Reasonable use of computer facilities for personal correspondence, where not connected with any commercial activity, is at present regarded as acceptable.

Prior permission from the Technical Director / Manager, must be obtained in writing if use could possibly fall outside of the terms defined above.

Any restrictions placed on the use of equipment administered by Hazelwood Schools must be observed.

No person or persons shall use Hazelwood Schools' information systems to hold or process personal data except in accordance with the provisions of the Data Protection Act 1998. Any person wishing to use the facilities to hold or process personal data shall be required to inform in advance the Data Protection Officer administering the appropriate computer facility, to comply with any restrictions Hazelwood Schools may impose concerning the manner in which the data may be held or the processing carried out.

All use of the facilities shall be lawful, honest and decent, and shall have regard to the rights and sensitivities of other people.

Breaches of these Rules are offences under the rules of Hazelwood Schools and are punishable under these rules. If after investigation it appears prima facie that a member of Hazelwood Schools has acted in breach of these rules, he or she may be denied access to all computer facilities pending the conclusion of disciplinary proceedings against him or her.

APPENDIX 1 GUIDANCE ON E-MAIL USE

Sending mail

Do not send e-mail which is abusive or in any other way offensive, harassing, etc.

Do not send "broadcast" messages.

Do not attempt to send spam messages advertising or promoting things.

Don't send mail to people whom you don't know, unless there is a good academic reason for doing so.

Always fill in the Subject header in your message.

Always reread a message before sending it, and check the To: and Cc: fields

Signatures

If you use an e mail signature, it should be brief (four or five lines maximum) and informative.

Chain letters

Do not send e mail chain letters, and do not forward such messages.

If you forward spam or chain letters to anyone else, here or elsewhere, your user account can be disabled and you may be subject to disciplinary procedures.

Reading mail

Read your school mail frequently (daily if possible, at least weekly).

Delete messages that you don't need to retain. More importantly, delete any attachments that came with them.

a e note of the require ent to co p y w th the Obscene Pub cat ons Act. If so eone sends you f e as an attach ent that you suspect w contravene the Act you shou d de ete t ed ate y. If you have any probe de et ng such a f e not fy Co put ng s erv ces ed ate y. If you fa to act you ay be ab e even f you d d not request that the f e be sent to you.

Receiving messages you didn't want

Junk mail ("spam") is common in the Internet. If you receive junk mail, delete it and forget it. You may be the only recipient in the "To:" header, and you may get the feeling that you are being addressed personally: that's the object - don't be fooled.

Do not reply to junk mail, even if asked to do so in order "to be removed from this mailing list". The sender's program is trying to establish how many people actually exist, of the thousands to whom it has sent the message.

E-mail lists (bulletin boards, forums, etc.)

When replying to mail that has been sent to a list, decide whether your reply should be to the sender only, or whether everyone on the list should see it.

Having composed your reply, check the To: and the Cc: headers. Once an e mail has been sent, it cannot be retrieved.

Never, never send an attachment to an e-mail list.

Finally, if you receive e-mail which upsets you in some way (for example it is abusive, pestering, or another form of harassment), report it to IT Support or call into the office.

APPENDIX 2 GUIDANCE ON COMPUTER MISUSE ACT

- .Introduction
- .Definition
- .Action to deal with misuse
- .Summary
- .References

INTRODUCTION

The Computer Misuse Act became law in August 1990. Under the Act hacking and the introduction of viruses are criminal offences. Schools and colleges need to co-operate to take action under the Act as the offences are likely to be committed by members of schools and colleges, students in particular, and are often perpetrated on machines or networks within the sector. For offences committed within the higher education sector institutions may wish to use the speedier process of internal disciplinary measures rather than resort to the law. The aim of this Guidance is to ensure that schools recognise the seriousness of these offences and to encourage a greater degree of common practice in dealing with the people who carry out these actions, whether action is taken under the criminal law or through the use of disciplinary procedures.

The following sections describe the types of offence and suggest a range of internal penalties.

DEFINITION

The Act identifies three specific offences"

1. Unauthorised access to computer material (that is, a program or data)
2. Unauthorised access to a computer system with intent to commit or facilitate the commission of a serious crime.
3. Unauthorised modification of computer material

The Act defines (1) (the basic offence) as a summary offence punishable on conviction with a maximum prison sentence of six months or a maximum fine of 2000 or both. The Act goes on to describe offences (2) and (3) as triable either summarily or on indictment, and punishable with imprisonment for a term not exceeding five years or a fine or both. These sentences clearly reflect the perceived gravity of the offence and would imply that schools should take an equally serious view of hacking or virus proliferation.

Schools are primarily concerned with preserving the integrity of shared academic computer systems and of all administrative systems. In the event of any problem information systems managers would expect to take immediate remedial and preventive action and would expect the institution to back them up in this action with penalties in place which would serve to discourage hacking, particularly the third category which could result in a student's work being destroyed or in a complete system failure.

Definitions of Unauthorised Access in the Higher Education Context

The offences described in the Act can be interpreted within the schools scene and perhaps extend into areas which in the wider context would not be considered to be offences. The examples given below are intended as a guide to the seriousness of the offence and do not attempt to cover all eventualities.

Example 1, Unauthorised Access to Computer Material.

This would include: using another person's identifier (ID) and password without proper authority in order to use data or a program, or to alter, delete, copy or move a program or data, or simply to output a program or data (for example, to a screen or printer); laying a trap to obtain a password; reading examination papers or examination results.

The response to some actions will depend on the specific conditions of use in force. Take, for example, unauthorised borrowing of an identifier from another student in order to obtain more time for a computer project the student was required to complete. In this case both the student who borrowed the ID and the student who lent it would be deemed to have committed an offence.

Example 2, Unauthorised Access to a Computer with intent.
This would include: gaining access to financial or administrative records, but intent would have to be proved.

Example 3, Unauthorised Modification of Computer Material.
This would include: destroying another user's files; modifying system files; creation of a virus; introduction of a local virus; introduction of a networked virus; changing examination results; and deliberately generating information to cause a complete system malfunction.

Schools should recognise that action under disciplinary procedures is more effective if a similar view is taken across the sector and if institutions are prepared to discipline their students for offences carried out across the network on the facilities of other schools.

It is desirable that as far as possible similar offences in different institutions carry similar penalties.

ACTION TO DEAL WITH MISUSE

.Preventive Measures

The simplest form of preventive action is publicity, and all opportunities should be used to make it clear that the universities and colleges do not tolerate this type of behaviour.

The conditions of use for computing facilities should spell out the seriousness of these activities.

.Preliminary Action

The status of the senior managers responsible for information systems can vary from one institution to another. It is assumed that in every university such senior managers have the authority to suspend access to the facilities for which they are responsible. The institution should support such action and ensure that managers with responsibility for local systems have the knowledge and the authority to take similar action. Such suspension of access would be a likely initial response to any misuse.

.Computer Security

The then Computer Board circulated to universities in March 1989 advice on measures to combat hackers. With the Computer Misuse Act coming into force these measures assume even more importance.

.Identifying the Offender

Finding and identifying someone who has hacked into or misused a system is a difficult and, above all, time consuming task. It is sometimes possible to identify the person uniquely. More often it relies on producing sufficient circumstantial evidence to persuade the offender to admit that he perpetrated the offence.

Penalties under the Disciplinary Procedures

Care needs to be taken when assessing the level of punishment. Schools disciplinary procedures may not need the strict proof required by criminal law and thus may need to consider only the balance of probabilities. However, institutions should ensure that the standard disciplinary procedures do satisfy the requirements of natural justice. A narrow line needs to be taken between making the penalties so severe that they are never implemented and being so lax that hacking and other misuse is treated as just a game.

The least serious offences could be punished solely by temporary withdrawal of the facilities together with a formal warning from an appropriate person, such as tutor or head of

department for a student or line manager for a member of staff. However, such a warning must be recorded, as a second offence clearly becomes much more serious.

The next point on the scale could be a fine, for those universities which use such systems, or a fixed period, set at an appropriate level, of withdrawal of access to computing resources.

For the more serious offences of category (2) and category (3) the minimum penalty should be withdrawal of all computing resources for a term but the normal penalty should clearly be more severe and commensurate with the degree of intent and seriousness of the offence. The consequential effects of withdrawal of facilities should be borne in mind, including the fact that consequential effects will vary in each case. For example, withdrawal could have the effect of forcing a student to repeat examinations or to repeat a year. If the person has already been warned, or if the disruption is intentional or severe, then more severe penalties should be invoked. For a student it is suggested that they should not be allowed to continue the course.

Initiating Legal Procedures

Schools should be prepared to use the full powers of the Act for serious offences whether they originate within or without the higher education sector. It is normally the responsibility of the Police to initiate any action, but for a prosecution to be successful, evidence needs to be collected and kept as soon as misuse is suspected. Schools could well need to seek technical and legal advice early in the proceedings.

SUMMARY

1. The definitions of computer misuse in the Act should be used.
2. A range of penalties, matched to the offence, should be recognised, from suspension of use of computer facilities for varying lengths of time, through fines to the ultimate sanction of being sent down; legal sanctions should be invoked where appropriate.
3. Second and subsequent offences should be treated increasingly more severely than first offences.

4. Offences committed on the facilities of other institutions should be treated at least as severely as offences committed on local machines.

References.

1. Computer Misuse Act 1990 Chapter 13 BN 0 0 5 000.
2. Computer Board paper. Specific Measures to Combat Hacking,

APPENDIX II Note: The following principles are contained within the Data Protection Act.

1. The information to be contained in personal data shall be obtained,
and personal data shall be processed, fairly and lawfully.
2. Personal data shall be held only for one or more specified and lawful purposes.
3. Personal data held for any purpose or purposes shall not be used or disclosed in any manner incompatible with that purpose or those purposes.
4. Personal data held for any purpose or purposes shall be adequate, relevant and not excessive in relation to that purpose or those purposes.
5. Personal data shall be accurate and, where necessary, kept up to date.
6. Personal data held for any purpose or purposes shall not be kept for longer than is necessary for that purpose or those purposes.
7. An individual shall be entitled -
 - a. at reasonable intervals and without undue delay or expense -
 - i. to be informed by any Data User whether he holds personal data of which that individual is the subject;
 - ii. to have access to any such data held by a Data User;
 - and
 - b. where appropriate, to have such data corrected or erased.
8. Appropriate security measures shall be taken against unauthorised access to, or alteration, disclosure or destruction of, personal data and against loss or destruction of personal data.