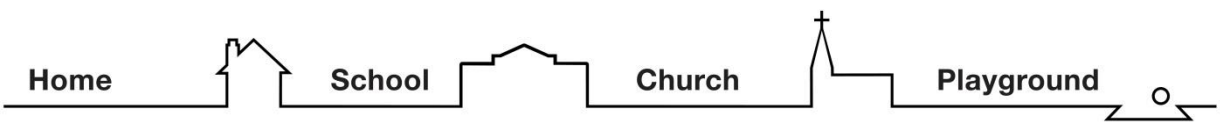
Thornleigh Salesian College

E-Mail, Internet Security and Facsimile Security Policy

Reviewed by:	Bolton LA
Last Reviewed:	September 2013
Adopted by Governing Body:	9th April 2014



CONTENTS

		Page No
1.	Introduction	**1**
2.	Guiding Principles	**1**
3.	Appropriate and Inappropriate Use of Information Systems	**2**
4.	Copyright & Licensing	**3**
5.	Etiquette and User Responsibilities	**3**
6.	Utilisation, Retention and Deletion of Files	**4**
7.	Monitoring	**5**

APPENDICIES

1.	Email, Internet Security & Facsimile Policy Do's and Don'ts	**7**
2.	School Disclaimer	**8**
3.	Email, Internet Security & Facsimile Policy Declaration	**9**

1. INTRODUCTION

1.1 The increasing use of Information and Communications Technology necessitates a security policy to ensure these systems are developed, operated and maintained in a safe and secure manner.

1.2 The Internet is the single most significant and unique development in information technology in recent years. It has evolved into a world-wide open environment of networked PCs and computer services, whose whole purpose is to facilitate the open exchange of information. The Internet can be utilised to provide significant business benefits, particularly in respect of promoting the School's image to the outside world. However, it's very openness makes it vulnerable to security threats, and appropriate controls are required to minimise these risks.

1.3 The Policy will apply to all staff who need to be aware of the importance of information security and their responsibilities for security whilst working in School premises or off site.

1.4 It is not the intention of the Policy (or resultant security controls) to be unnecessarily restrictive. The aim of the Policy is to ensure there is a framework of control in place for mitigating significant risks to the School's information services, its employees and its image.

1.5 The Policy is binding on all employees who are authorised to use email, the Internet or the facsimile systems for School business and **must** be adhered to at all times.

2. GUIDING PRINCIPLES

2.1 The Policy has been drawn up having regard to the following guiding principles:

- To outline the strategic framework and responsibilities for maintaining effective security over the School's Internet, email and facsimile systems.

- To ensure appropriate levels of:

  i. **Confidentiality** - ensuring information is not disclosed inappropriately.

  ii. **Integrity** - safeguarding the validity, accuracy and completeness of information owned, obtained and used by the School.

  iii. **Availability** - ensuring that information is accessible and usable when required for the business of the School.

  iv. **Relevance** - ensuring that the Internet, email and facsimile systems are used in accordance with the business needs of the School.

2.2 The Policy has been drawn up in accordance with current statutory provisions relating to information systems including:

- The Regulation of Investigatory Powers Act 2000
- The Freedom of Information Act 2000
- The Data Protection Act (UK) 1998
- The Computer Misuse Act 1990
- Copyrights, Designs and Patents Act 1988
- The Obscene Publications Act 1959 and 1964
- Equality Act 2010

3. APPROPRIATE AND INAPPROPRIATE USE OF INFORMATION SYSTEMS

3.1 Communication resources belong to the School and are to be used solely for School business. However, where an employee has access to the equipment out of business hours and/or has obtained appropriate permission to use the equipment, and where there is no extra cost to the School, employees are encouraged to develop their skills, knowledge and understanding of the email and Internet as long as these systems are used reasonably and appropriately.

As a general principle, Internet access, email and facsimile facilities are provided to employees to support them in their work related activities. The following list, although not intended to be definitive, sets out broad areas of use that the School considers to be appropriate:

- to provide a means of business communication within the School and other Schools, agencies and organizations;
- to view and obtain information in direct support of the School's business activities;
- to promote services and products provided by the School;
- to communicate and obtain information in support of approved personal training and development activities;
- any other use that directly supports work related functions.

It is each employee's responsibility to check with their Head Teacher to ascertain whether any proposed use, not referred to in the above paragraph, falls within the School's definition of appropriate use.

3.2 The use of the School's systems to communicate Trade Union business is laid down in the *School's Facilities Agreement: Time off for Trade Union Duties and Activities.*

3.3 Any abuse or misuse of the School's communication resources by an employee may be considered a disciplinary offence.

3.4 Some examples of what could constitute a disciplinary offence under the Policy are:

- Contravention of a legal provision, e.g. The Regulation of Investigatory Powers Act 2000; The Freedom of Information Act 2000, The Data Protection Act 1998; The Computer Misuse Act 1990; The Copyrights, Designs and Patents Act 1988; The Obscene Publications Act 1959 and 1964; or any internal Council policy (in particular, Council policies on Valuing Diversity) is unacceptable; See also separate school policy for Use of Social Networking Sites.
- use of equipment without prior consent;
- circulation of personal information, for example advertisements, offers to sell goods, etc;
- introduction of viruses;
- viewing, downloading and/or circulating illegal or offensive material from the Internet;
- unauthorised viewing of other people's emails;
- use of email for potential offensive or defamatory purposes;
- hacking into other people's emails and systems;
- unauthorised alteration of data;
- circulation of malicious/racist/sexist/offensive material including chain letters.

3.5 Employees should be aware that any of the above could also constitute a criminal offence.

4. COPYRIGHT & LICENSING

4.1 All employees are responsible for ensuring that copyright and licensing laws are not breached. If in doubt you can seek advice from Local Authority Legal Services.

5. ETIQUETTE AND USER RESPONSIBILITIES

5.1 Employees need to be mindful that they are acting as representatives of the School when using School equipment.

5.2 Whilst employees can expect the School to respect their privacy there are certain exceptions, in relation to the communication systems where staff should be aware that there is routine monitoring by the School (see Section 7 Monitoring).

5.3 Although each employee has a password to his/her computer, this does not guarantee private viewing. Hackers can enter networks, information transmitted can also be captured by other Internet sites.

5.4 Head Teachers should seek to ensure that the Internet and email is used appropriately and in direct relation to the work of an employee. Head Teachers should make employees aware of the potential addictive qualities of the Internet and the use of computers in general.

5.5 Head Teachers should ensure, through the Personal Development Plan process that appropriate training is made available to employees who have access to Council's information and communication systems.

5.6 Head Teachers are responsible for ensuring employees understand their rights and responsibilities with regard to the use of the School's communication systems. Head Teachers must ensure employees receive a copy of this Policy and any subsequent amendments, along with a copy of the Employee Declaration, attached at Appendix 3.

5.7 Employees should be aware that leaving their password by their terminal or leaving their terminal on overnight renders security systems ineffective. Employees should therefore ensure that terminals are switched off at the end of the working day and passwords are kept secure.

5.8 Employees who have access to lap tops, and any other mobile equipment, are responsible for the safety and security of any such equipment.

5.9 Employees should be familiar with the contents of this Policy.

5.10 Employees should be aware that an email, or fax, can constitute a contract. Therefore it is the responsibility of each employee to ensure that the content of emails, and faxes, are correct, whether they are sending or receiving emails or faxes.

5.11 Employees must ensure that they do not deactivate or invalidate the disclaimer (at Appendix 2) from their systems.

5.12 Employees must ensure they do not deactivate the virus scanners on their systems.

5.13 If an employee unintentionally accesses an Internet site which contains material of an offensive or undesirable nature, he/she should immediately exit the site. In such a situation an employee should report the incident to his/her Head Teacher who may prevent future access to such sites by implementing preventative measures having consulted with Schools' ICT. Sites relating to sex, gambling etc are routinely recorded and reported to Head Teachers *(as applicable).*

6. UTILISATION, RETENTION AND DELETION OF FILES

6.1 Emails and faxes are a form of publication. Employees as well as the School are potentially open to action for libel, defamation or breach of trust.

6.2 Whenever an external email is sent an employee's name, job title and email address must be included on the email. The Disclaimer, attached at Appendix 2, will automatically be included on external emails. All faxes must detail the employee's name, fax and telephone number and School's address on the cover sheet accompanying the fax.

6.3 Employees need to be aware when composing emails or faxes that messages can easily be misconstrued and therefore the message being transmitted should be accurate and relevant to the recipient.

6.4 Forgery or attempted forgery of electronic mail is prohibited at all times.

6.5 Head Teachers will have access to emails where staff are absent on leave or through sickness. Emails are not a private means of communication but a record on behalf of the School of work related matters.

6.6 If an employee receives an email or fax from outside the School that is considered to be offensive or malicious then he/she must consult his/her Head Teacher. In such circumstances these emails or faxes should not be responded to.

6.7 It is important to remember that an email or fax is not private. Email documents, and faxes, form part of the administrative records of the School and Head Teachers have the right of access to all emails, or faxes, sent or received, on the same basis as any other written documentation.

6.8 In order to ensure compliance with the requirements of the School and the contents of this Policy, monitoring software may be utilised to check on the use of email and Internet services, as well as software to check the content of email messages sent and received.

These software tools will only be used for the legitimate purposes of ensuring compliance with stated legal acts, policies and guidelines so as to protect the School against the risk of criminal and civil actions, as a result of the unauthorised actions of its employees, and in connection with the administration of the email and Internet service itself.

Employees should be aware that email messages, or faxes, could ultimately be required to be disclosed in Court.

6.9 Employees are responsible for ensuring hard copies of formal communications are made and stored or filed in accordance with School requirements and where appropriate statutory requirements. Formal documents can include emails, or faxes, that replace letters, confirmation, agreements, requests for information, etc. If in doubt employees should seek guidance from the Head Teacher.

6.10 Email communications and records held by or on behalf of the School may be subject to the Freedom of Information Act, so that anyone may be entitled to access to them, unless exempt from disclosure under the Act. School's ICT Unit within Children's Services can advise further if necessary.

7. MONITORING

7.1 The School, when monitoring, will ensure it complies at all times with the relevant legislation and guidance, including:

- The Regulation of Investigatory Powers Act 2000
- The Freedom of Information Act 2000
- The Data Protection Act 1998
- The Human Rights Act 1998
- The Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000

7.2 The Regulations allow business and public authorities to record or monitor communications without consent in such cases as:

- recording evidence of transactions
- ensuring compliance with regulatory or self regulatory rules or guidance
- gaining routine access to business communications
- maintaining the effective operation of the systems
- monitoring standards of service and training, and
- combating crime and the unauthorised use of systems

The School reserves the right accordingly to monitor email communications and records without notice.

APPENDIX 1

Thornleigh Salesian College

SCHOOL EMAIL, INTERNET SECURITY & FACSIMILE POLICY

Worldwide the email and Internet are increasingly used as a means of communication along with the use of faxes.

Whether you use these systems or not, you should be aware that we all represent the School and are accountable to the public.

Therefore to ensure the protection of the School, its employees and all other authorised users, the School's Email, Internet Security and Facsimile Policy has been produced. The Policy makes it a disciplinary offence to abuse or misuse the School's communication and information systems.

The Policy is binding on all employees and users of the systems. Access to the full document can be gained through the Head Teacher.

As an Employee you have a responsibility for the way you use the School's email, internet and telecommunication systems. The information below covers the main do's and do not's you need to be aware of.

DO:

- ✓ Be aware that telecommunication systems will be monitored when it is necessary and appropriate
- ✓ Respect the confidentiality of the School and of those who send you information
- ✓ Respect password privacy and be vigilant of 'hackers'
- ✓ File and store information correctly and safely
- ✓ Be aware of the addictive qualities of the 'Net'
- ✓ Take advantage of the appropriate training
- ✓ Discuss with your Head Teacher any issues you may have, and if necessary ask for a copy of the Policy
- ✓ Ensure lap tops and any other mobile equipment is kept secure at all times
- ✓ Ensure appropriate use of language as email and fax messages can be misconstrued

DO NOT:

- X Infringe copyright and licensing laws
- X Distribute material containing offensive language, offensive images or chain letters
- X 'Hack' into files you are not authorised to access
- X Store obsolete and out of date information
- X Access inappropriate websites
- X Use the School's resources without permission

APPENDIX 2

Thornleigh Salesian College

SCHOOL EMAIL, INTERNET SECURITY & FACSIMILE POLICY

DISCLAIMER

This email and any attached files are confidential and may also be legally privileged. They are intended solely for the intended addressee. If you are not the addressee please email it back to the sender and then immediately, permanently delete it. Do not read, print, re-transmit, store or act in reliance on it. This email may be monitored by the School in accordance with current regulations.

This footnote also confirms that this email message has been swept for the presence of computer viruses currently known to the School. However, the recipient is responsible for virus-checking before opening this message and any attachment.

Unless expressly stated to the contrary, any views expressed in this message are those of the individual sender and may not necessarily reflect the views of the School.

APPENDIX 3

Thornleigh Salesian College

SCHOOL EMAIL, INTERNET SECURITY & FACSIMILE POLICY

DECLARATION

I confirm that I have received a copy of the School's Email, Internet Security and Facsimile Policy.

I have read and understood the Policy and am aware that should I contravene the requirements contained in the Policy disciplinary action may be taken.

NAME:.....

Class/Faculty:.....

EXTENSION:.....

SIGNED .....

DATE: .....

HEAD TEACHER'S SIGNATURE:.....

DATE:.....

Please send your completed declaration to your head teacher.