



## NETWORK, INTERNET & EMAIL ACCEPTABLE USE POLICY

### AIM OF THE HARRIS MIDDLE SCHOOL

The aim of Harris Middle School is to provide an excellent education in a safe, supportive learning environment, where people are valued and make positive contributions to the learning community, and where students enjoy and achieve and go on to attain social and economic well-being as responsible, independent members of society.

The IT Manager will be designated by the Headteacher and have responsibility for the use of all ICT resources around the school. They will take the lead for ICT across the curriculum and support the use of ICT for administrative purposes. They will also have primary responsibility for the Acceptable Use Policy (AUP) and its adherence by all staff, students and members of the learning community.

The IT Network Manager will be responsible for the provision and maintenance of all identified ICT resources required by the school. They will take the lead in maintaining the integrity and security of these resources in line with “best practise” and statutory requirements.

### 1. PRINCIPLES

We believe that staff and students at Harris Middle School have the right to work and study using the internet, intranet, & network within the school in a safe learning environment. Access to these resources must be within the law.

### 2. PURPOSES

2.1. The policy defines and describes the use of the IT network and electronic information to support, enhance and develop all aspects of the curriculum at Harris Middle School.

2.1.1. To ensure that all users have full use of all resources allocated to them from any computer within their scope of access.

2.1.2. To ensure that all users are able to access the internet in order to support and promote learning.

2.1.3. To provide all users with a secure environment in which to use network and internet resources.

### 3. OBJECTIVES AND SCOPE

3.1. The primary objectives of this policy are:

3.1.1. to safeguard IT resources and the integrity of data stored on them;

3.1.2. to minimise the liability arising from the misuse of IT resources and data;



3.1.3. to ensure that the confidentiality of data is protected to the extent allowed or required by all laws pertaining to it.

3.2. The policy detailed here applies to the use of all IT resources and data and is applicable to all staff and students of Harris Middle School, and all other authorised users.

## 4. TCC RESPONSIBILITIES

4.1. All IT systems, resources & data are the property of Harris Middle School and Suffolk County Council, including laptops & mobile computing devices, software, operating systems, storage media and network accounts that provide access to local, network, and internet and email resources.

4.2. Harris Middle School will ensure that all users are fully aware of the contents contained within this policy.

4.3. The IT Department is responsible for granting access to IT resources allocated to staff and students in accordance with their role within the school. Any deviation from this must be authorised by the Head Teacher in writing or electric email in accordance with the Data Protection Act 1998.

4.4. When a breach of this policy is reported, the incident will initially be reviewed by the IT Manager and passed to either the Headteacher or relevant Head of Year for further review in accordance with the Student Behaviour Policy or Staff Disciplinary Procedures.

4.5. Within the terms of the Data Protection Act 1998, Human Rights Act 1998 and the Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000, Harris Middle School may record or inspect any information transmitted through or stored in its IT resources, including e-mail communications, Voicemail and individual login sessions, without notice when:

4.5.1. There is reasonable cause to believe the user has violated or is violating this policy, any guidelines or procedures established to implement this policy.

4.5.2. An account appears to be engaged in unusual or unusually excessive activity.

4.5.3. It is necessary to do so to protect the integrity, security, or functionality of IT resources or to protect Harris Middle School from liability.

4.5.4. Establishing the existence of facts relevant to the business.

4.5.5. Ascertaining or demonstrating standards which ought to be achieved by those using the IT facilities

4.5.6. Preventing or detecting crime

4.5.7. Investigating or detecting unauthorised use of IT facilities

4.5.8. Ensuring effective operation of IT facilities

4.5.9. Determining if communications are relevant to the business (for example, in the last resort where an employee is off sick or on holiday and business continuity is threatened)

4.5.10. It is otherwise permitted or required by law.



## 5. USER RESPONSIBILITIES

- 5.1. When using computer network and internet resources all users must comply with all laws pertaining to their access, including copyright, libel, fraud, discrimination and obscenity laws.
- 5.2. All breaches of this policy must be reported to the IT Manager or IT Network Manager in the first instance.
- 5.3. By logging onto or using any IT resource belonging to or within the boundaries of Harris Middle School, users agree to abide by this policy and all policies and laws relating to the use of IT.
- 5.4. All staff and students are to act in a responsible, lawful and ethical manner. Staff must be aware that all data including electronic email and documents stored on the system may be accessible to the public under the freedom of Information Act 2000.
- 5.5. All users must agree to comply with the provisions of the following Acts of Parliament:
  - 5.5.1. Computer Misuse Act 1990
  - 5.5.2. Copyright, Designs and Patents Act 1988
  - 5.5.3. Crime and Disorder Act 1998
  - 5.5.4. Data Protection Act 1998
  - 5.5.5. Privacy and Electronic Communications (EC Directive) Regulations 2003
  - 5.5.6. Protection from Harassment Act 1997
  - 5.5.7. Protection of Children Act 1976, as amended by Sect 84 of the Criminal Justice and Public Order Act 1994
  - 5.5.8. Children Act 1989 and 2004
  - 5.5.9. Malicious Communications Act 1988
  - 5.5.10. Sexual Offences Act 2003
  - 5.5.11. The Obscene Publications Act 1959 and 1964
  - 5.5.12. The Telecommunications Act 1984
- 5.6. All users are to ensure that their password is not shared or compromised, nor use another users account or attempt to access another user account. If a user's password is found to be compromised, it is the responsibility of the user to ensure that their password is changed following current guidelines.
- 5.7. Users shall not access another users personal electronic document (email included) without the owners express permission or as allowed by law.
- 5.8. Staff are to ensure that no computer resource allocated to them is left unsecure where there is student access.
- 5.9. Staff are not permitted to use portable hard drives or any removable media without prior agreement of the IT Network Manager.
- 5.10. Students are not permitted to use portable hard drives or any removable media unless under supervision and with the knowledge of the IT Network Manager.
- 5.11. No person may knowingly:
  - 5.11.1. Copy, save or redistribute copyright-protected material, without approval, this includes music & video files.



- 5.11.2. Connect a device to the network or any IT resource without prior approval, this includes VOIP phones, laptops, PDAs, Gaming devices, mobile phones.
  - 5.11.3. Play online computer games or use interactive 'chat' sites unless specifically approved by the school.
  - 5.11.4. Access social networking sites unless specifically approved by the school.
  - 5.11.5. Use the network in such a way that the use of the network by other users is disrupted (for example: downloading large files during peak usage times; sending mass email messages).
  - 5.11.6. Retrieve, send, copy or display offensive, pornographic, obscene or racist messages or pictures.
  - 5.11.7. Use obscene or racist language, or harass, insult or attack other people
  - 5.11.8. Damage computers, computer systems or computer networks.
  - 5.11.9. Use another user's password.
  - 5.11.10. Create or transmit any offensive, obscene or indecent images, data or other material, or any data capable of being resolved into obscene or indecent images or material;
  - 5.11.11. Create or transmit defamatory material
  - 5.11.12. Corrupt or destroy other users' data;
  - 5.11.13. Disrupt the work of other users;
  - 5.11.14. Introduce or attempt to introduce a "virus".
  - 5.11.15. Attempting to bypass network or computer security including Antivirus Software, using programmable scripts or network monitoring software.
  - 5.11.16. Attempt to gain access to or use resources NOT allocated to them.
  - 5.11.17. Download programs without approval from the IT Manager.
  - 5.11.18. Use Peer to Peer file sharing programs (Kazaa, Emule, BitTorrent etc).
  - 5.11.19. Use MSN, Yahoo, AOL Messenger or other types of chat programs whilst connected to the school network.
  - 5.11.20. Use external web based email for school purposes (staff only), as this could breach the Data protection Act 1998 or the Children Act 2004.
- 5.12. Users should:
- 5.12.1. Inform the IT Manager, IT Network Manager or an appropriate member of staff if they believe that attempts have been made to use the internet in an unacceptable manner.
  - 5.12.2. Inform the IT Manager, IT Network Manager or an appropriate member of staff if they discover any materials they consider may be offensive or inappropriate.

## 6. INTERNET CONTENT FILTERING

- 6.1. It is an absolute requirement that access to the Internet provided to staff and students in any school or educational institution through any Internet Service Provider (ISP) is a filtered service.
- 6.2. All users should be aware that the Local Authority and IT Department staff at Harris Middle School can track and record the sites visited and the searches made on the Intranet/internet by individual users.



- 6.3. Parents should be aware that with the emerging and constantly changing technologies there is no absolute guarantee that users cannot access materials that would be considered unsuitable.
- 6.4. If a student or member of staff is unfortunate enough to come across any offensive web pages, whilst using school equipment, they should make a note of the address and report it to a designated member of staff immediately; this will normally be the IT Manager. The IT Manager will then take the appropriate action.

## **7. ADDITIONAL GUIDELINES FOR STAFF**

- 7.1. Under no circumstances are students permitted to use staff laptops unless under direct supervision of staff.
- 7.2. Students should be encouraged to use the internet and intranet where appropriate.
- 7.3. The IT Manager, with the assistance of the IT Network Manager, may review files and communications to maintain system integrity and ensure that users are using the system responsibly. While normal privacy is respected and protected by password controls, as with the Internet itself, users must not expect files stored on the Harris Middle School network to be absolutely private.
- 7.4. Staff are permitted to use the internet and intranet for their own non-school purposes during break and lunch times and before and after school. However, during the school day it is expected that use of the internet and intranet by staff will be solely to support teaching and learning or school administration.

## **8. DISCOVERY OF INCIDENTS INVOLVING ILLEGAL MATERIALS OR ACTIVITIES**

See Procedure H

## **9. DOWNLOADING AND INSTALLING SOFTWARE**

- 9.1. Only members of Harris Middle School IT Department are allowed to download and install software on college computers that is not on the approved list and on network resources without prior approval.
- 9.2. Students are NOT permitted to download and install software to any resource connected to the network or belonging to Harris Middle School
- 9.3. Staff wishing to download software MUST refer to the "Software Download Procedure"

## **10. EMAIL**

- 10.1. The use of email is governed under a separate procedure outlined in Appendix D.



## Appendix A Anti Virus Procedures

### Definitions

- a. Virus - A program that is designed to replicate.
- b. Macro virus - A virus that lives inside word or excel documents.
- c. Boot sector virus - A virus that lives on the boot sector of a floppy disk.
- d. Partition sector virus - A virus that lives on one of the partition sectors on a hard disk.
- e. File virus - A virus that lives inside an executable file (\*.exe, \*.com).
- f. Stealth - The level of visibility of the virus.

### Description

- a. All school workstations are to run the latest version of a virus protection programme. Currently this is AVG Anti Virus as provided by County IT Services.
- b. All users must be responsible for any infected files or disk brought into the school.
- c. If a Virus is discovered the infected computer **MUST** be switched off Immediately and the IT Manager or IT Network Manager informed
- d. File servers, PCs, Laptops and USB memory devices are to be scanned on a regular basis and any viruses removed.
- e. Users should be educated about computer viruses.
- f. Regular backups should be made of all file servers, PCs and laptops, and critical workstations.
- g. Only software from reputable sources should be installed onto workstations and or file servers under the supervision of the IT Network Manager.
- h. File servers should run anti virus software to stop any new viruses bypassing the workstation anti virus software.
- i. Users should only have restricted access to file servers to minimise the spread of viruses across file servers.
- j. The Internet should not be trusted as a virus free source of files.

### Related procedures

File server backup procedure in Appendix B.



## Appendix B Server Backup Procedures

### Purpose

This procedure is to ensure that the school has adequate and secure backups of all systems to enable a full recovery to be carried out in an emergency or a partial recovery on request.

### Scope.

This applies to all servers in use throughout the school by all academic and support staff.

### Responsibility

The staff in the IT Department are responsible for the day to day operation of this procedure. Overall responsibility is with the IT Network Manager.

### Definitions

Full System Backup is defined as a complete Tape copy of the system.

### Description

There are three servers, which require backing up.

- a. Collect 1 x Tape from the school Bursar and 1 x Tape from the IT Network Manager
- b. Use Master Key to access the Server room door
- c. Check to see if the tapes have ejected from the tape drives
- d. If a tape has not ejected go to 6.d.i otherwise go to 6e
  1. Access log onto the server
  2. Access Veritas Backup Exec
  3. Ascertain by checking the logs why the backup tape did not eject
  4. Inform the IT Manager that the Backup has failed
  5. Carry out any remedial action to rectify any faults
- e. Replace the two tapes in the backup drives and removed tapes, one to the School Bursar in the school office and the second tape to the IT Network Manager. In case of a Fire Alarm be ready to remove them on evacuation.
- f. At the end of the working day the removed tapes are to be stored off site at the School Bursar's and IT Network Manager's residences.
- g. If there are five weeks in the month, then on the fourth Friday use Friday 4. On the fifth Friday use the Month tape.
- h. All tapes are marked with the appropriate name followed by day or month.
- i. Admin Tuesday



j. Admin Friday 2

k. Admin January

## Selecting Backup Tapes

The tapes are changed as per the tape backup generation below.

Week	Day	Tape Used
1	Monday	Monday
1	Tuesday	Tuesday
1	Wednesday	Wednesday
1	Thursday	Thursday
1	Friday	Friday 1
2	Monday	Monday
2	Tuesday	Tuesday
2	Wednesday	Wednesday
2	Thursday	Thursday
2	Friday	Friday 2
3	Monday	Monday
3	Tuesday	Tuesday
3	Wednesday	Wednesday
3	Thursday	Thursday
3	Friday	Friday 3
4	Monday	Monday
4	Tuesday	Tuesday
4	Wednesday	Wednesday
4	Thursday	Thursday
4	Friday	Friday 4 or Month

## Tape cleaning

Tape drives– these require cleaning on a monthly basis or when the ‘Use Cleaning Tape’ light comes on.

## System recovery

A test restore from backup is to be carried out on a monthly basis unless a recovery has occurred during that month. A log is to be kept and signed by the School Bursar and the IT Network Manager who both witnessed the restores.

## Data Security

Backup Tapes are not to be removed from site without prior permission of the IT Manager. Any tape removed from site by persons other than the IT Network Manager must be approved by either the IT Manager or the Headteacher and signed for.



## Appendix C IT Disaster Recovery Procedures

### Purpose

This document underlines the principle goals and steps taken to achieve those goals within the bounds of disaster recovery.

### Scope

The procedure applies to all school IT equipment.

### Responsibility

The staff in the IT Department are responsible for the day to day operation of this procedure. Overall responsibility is with the IT Manager.

### Applicable To

The IT Department.

### Definitions

Types of Disaster

- i. A hard-drive down;
- ii. A network card down;
- iii. A single server damaged or destroyed;
- iv. A single raid-stack damaged or destroyed;
- v. Multiple servers damaged or destroyed;
- vi. All servers destroyed and complete loss of IT Unit as would result from a fire.

### Description

Contingency Plan - Taken in order of severity the contingency for each event is described below.

- a. Hard-drive down:
  1. All servers have on-line spares, which can automatically recreate the failed drive onto an online spare.
  2. The servers can cope with a single drive failure, but a replacement of the failed drive would need to take place in order to preserve the contingency.
- b. A network card down:
  1. The servers should have multiple network cards installed if this is an option.
  2. There should be replacement network cards stored on-site.



- c. A single server destroyed or damaged:
  - 1. Backup servers should be available to replace any of the servers in event of a hardware failure.
- d. A raid stack damaged or destroyed:
  - 1. Spare disks packs should be kept on-site to replace a failed stack.
  - 2. Spare controller cards or maintenance contracts in case of controller failure.
- e. Multiple servers damaged or destroyed:
  - 1. If multiple servers are down and there are insufficient spare servers to replace them all then the plan is to prioritise the servers, this is a dynamic procedure and so speculation at this time is irrelevant. Needless to say the highest priority server is replaced by the contingency machine/machines. For contingency purposes any high spec PC could be configured as a replacement server but time to configure it would be the problem.
  - 2. Outsource from a disaster recovery company.
- f. Complete loss of I.T. Section as would result from a fire. All servers, network and on site data storage destroyed.
  - 1. Full backup tapes are stored off site each month.
  - 2. Outsource hardware from a disaster recovery service.

## Standard Procedures

- 1. As part of the Disaster Recovery Procedure there are a number of issues that must adhered to.
- 2. The emergency repair disks for all the Windows 2003 servers are kept up to date and in a secure location.
- 3. The Procedures for recovery are correct and up to date.
- 4. All IT Department staff are trained in the recovery procedures.
- 5. All primary systems should be protected by Uninterrupted Power Supplies (UPS). All Servers, Raid stacks and Network hardware should be plugged into UPSs. The UPS should be able to support the hardware long enough to allow the servers to be shutdown cleanly. More importantly the UPS protects the equipment from power spikes which can occur even in clean power supplies and will offer some protection from other types of power fluctuations such as lighting, which can induce large power bursts in the electric cables. UPSs need to be maintained.
- 6. The working environment in the computer rooms should facilitate work not hamper it. Rooms and equipment should be organised and tidy.



7. Software media should be secure and easy to locate. Time need not be wasted in a disaster situation looking for a specific driver or utility. To aid this, a catalogue system needs to be in place and maintained.



## Appendix D Email Procedures

### **Purpose**

This Email Procedure has been developed in response to the acknowledged need for guidelines describing the acceptable use of the school's email and related services and facilities.

The Procedure also describes the standards that users are expected to observe when using these facilities for email, and ensures that users are aware of the legal consequences attached to inappropriate use of the facilities.

The Procedure is designed to advise users that their usage of facilities for email will be monitored and, in some cases, recorded. The Policy is also linked to the school's Internet Acceptable Use Policy for students and staff, and usage of email facilities in breach of the Policy may lead to appropriate disciplinary action being taken.

The Procedure also specifies the actions that the school will take in the investigation of complaints received from both internal and external sources, about any unacceptable use of email that involves school IT facilities.

### **Applicable to:**

All staff.

### **Scope of the Procedure**

This Email Policy applies to the use, for the purpose of sending or receiving email messages and attachments whilst using IT facilities provided by Harris Middle School.

### **Appropriate and Proper Use**

Harris Middle School supports the appropriate and proper use of the Internet, email, and related services and facilities that the school provides for its students, staff and other authorised users.

### **Acceptance of Policies, Procedures and Regulations**

It is a condition of use of IT and email facilities provided by Harris Middle School, by a student, member of staff or other authorised person, that the user agrees to be bound by the relevant school Policies Procedures and Regulations.

### **Monitoring Arrangements**

Harris Middle School will maintain appropriate monitoring arrangements in relation to all Internet, email and related services and facilities that it provides, and the school will apply these monitoring arrangements to all users.

These arrangements may include checking the contents of, and in some instances recording, email messages for the purpose of:

- a. ascertaining or demonstrating standards which ought to be achieved by those using the facilities;
- b. establishing the existence of facts relevant to the business;
- c. preventing or detecting crime;
- d. investigating or detecting unauthorised use of email facilities;



- e. ensuring effective operation of email facilities;
- f. determining if communications are relevant to the business, for example where an employee is off sick or on holiday.

The school does apply automatic message monitoring, filtering and rejection systems and denies transmission of messages with content that is unacceptable in the terms of this Procedure.

These monitoring arrangements will operate on a continual and continuing basis, with the express aim of monitoring compliance with the provisions of the school's Email Procedures and IT Regulations and for the purposes outlined above as permitted by The Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations Act 2000.

## **Disclaimers**

The school does arrange for an appropriate disclaimer to be appended to all email messages that are sent to external addresses from the school, in order to provide necessary legal protection.

### **a. Current Disclaimer**

"This message and any included attachments are property of Harris Middle School and are intended only for the addressee(s).

The information contained herein may include privileged or otherwise confidential information. Unauthorised review, forwarding, printing, copying, distributing, or using such information is strictly prohibited and may be unlawful. If you received this message in error, or have reason to believe you are not authorized to receive it, please promptly delete this message and notify the sender by email. For further information please contact the IT Department on the school main number which can be found on our website."

## **Action in the Event of a Breach of the Standards of Acceptable Use**

In circumstances where there is assessed to be a breach of the standards of acceptable use, as described above, the school will, as a first action, act promptly to prevent continuance or repetition of the breach, for example to withdraw any unacceptable materials. This action will be taken in accordance with the normal managerial arrangements, and will typically involve liaison between the appropriate members Line Manager and the IT Manager in the first instance.

Indications of non-compliance with the provisions of the Email Procedure will be investigated, as appropriate, in accordance with the provisions of the school's Disciplinary Procedures, as applicable to staff and students.

Subject to the findings of any such investigation, non-compliance with the provisions of the Email Procedure will lead to appropriate disciplinary action, which could include dismissal on the grounds of gross misconduct. Furthermore, publication of some materials may not only amount to a disciplinary offence, but also a criminal offence, in which case the issue will be reported to the police for them to take appropriate action.

## **Appropriate Use of the School Provided Services and Facilities**

The main purpose for the provision by the school of IT facilities for email is for use in connection with the teaching, learning, research, and approved business activities of the school.

IT facilities provided by the school for email should not be used:

- a. for personal use during work periods, full guidelines are listed at Section 12 of this procedure;



- b. for the transmission of unsolicited commercial or advertising material, chain letters, press releases, or other junk-mail of any kind, to other user organisations, or to organisations connected to other networks, other than where that material is embedded within, or is otherwise part of, a service to which the member of the user organisation has chosen to subscribe;
- c. for the unauthorised transmission to a third party of confidential material concerning the activities of Harris Middle School;
- d. for the transmission of material such that this infringes the copyright of another person, including intellectual property rights;
- e. for the deliberate unauthorised access to services and facilities accessible via Suffolk County broadband Network;
- f. for the unauthorised provision of access to school services and facilities by third parties;
- g. for activities that unreasonably waste staff effort or networked resources, or activities that unreasonably serve to deny service to other users;
- h. for activities that corrupt or destroy other users' data;
- i. for activities that disrupt the work of other users.

## **General Standards of Use**

IT facilities provided by the school for email should not be used:

- a. for the creation or transmission (other than for properly supervised and lawful research purposes) of any offensive, obscene or indecent images, data, or other material, or any data capable of being resolved into obscene or indecent images or material;
- b. for the creation or transmission of material which is designed or likely to cause annoyance, inconvenience or needless anxiety;
- c. for the creation or transmission of material that is abusive or threatening to others, or serves to harass or bully others
- d. for the creation or transmission of material that either discriminates or encourages discrimination on racial or ethnic grounds, or on grounds of gender, sexual orientation, marital status, disability, political or religious beliefs. Harris Middle School is committed to fostering a learning and working environment free of discrimination where everyone is treated with dignity and respect;
- e. for the creation or transmission of defamatory material;
- f. for the creation or transmission of material that includes false claims of a deceptive nature;
- g. for so-called 'flaming' i.e. the use of impolite terms or language, including offensive or condescending terms;
- h. for activities that violate the privacy of other users;
- i. for criticising individuals, including copy distribution to other individuals;



- j. for publishing to others the text of messages written on a one-to-one basis, without the prior express consent of the author;
- k. for the creation or transmission of anonymous messages, i.e. without clear identification of the sender;
- l. for the creation or transmission of material which brings the school into disrepute.

The Harris Middle School Senior Leadership Team will exercise its discretion in judging reasonable bounds within the above standards for acceptability of material transmitted by email. In the first instance reports of suspected breaches of the Acceptable Use Policy will be made to the IT Manager.

## **Preventing the Spread of Malicious Software (Viruses)**

Users of school IT facilities must take all reasonable steps to prevent the receipt and transmission by email of malicious software e.g. computer viruses.

In particular, users:

- a. must not transmit by email any file attachments which they know to be infected with a virus;
- b. must ensure that an effective anti-virus system is operating on any computer which they use to access school IT facilities;
- c. must not open email file attachments received from unsolicited or un-trusted sources.

## **Personal Use**

The main purpose for the provision by the school of IT facilities for email is for use in connection with teaching, learning, research, and approved business activities of the school.

The school permits the use of its IT facilities for email by students, staff and other authorised users for personal use, subject to the following limitations:

- a. a level of use that is reasonable and not detrimental to the main purpose for which the facilities are provided;
- b. priority must be given to use of resources for the main purpose for which they are provided;
- c. personal use must not be of a commercial or profit-making nature, or for any other form of personal financial gain;
- d. personal use must not be of a nature that competes with the school in business;
- e. personal use must not be connected with any use or application that conflicts with an employee's obligations to Harris Middle School as their employer;
- f. personal use must not be connected to any purpose or application that conflicts with the school's rules, regulations, policies and procedures;
- g. personal use must comply with the school's policies and regulations, in particular the Email Procedure.



In relation to the personal use of school IT facilities for email, if users are in any doubt about what constitutes acceptable and appropriate use, they should seek the advice and guidance, in the case of members of staff, of the IT Manager, and in the case of students, of their Group Tutor.

## Legal Consequences of Misuse of Email Facilities

In a growing number of cases involving the civil or criminal law, email messages (deleted or otherwise) are produced as evidence in a permanent written form.

There are a number of areas of law which apply to use of email and which could involve liability of users or the school. These include the following.

- a. **Intellectual property.** Anyone who uses email to send or receive any materials that infringe the intellectual property rights of a third party may be liable to that third party if such use is not authorised by them.
- b. **Obscenity.** A criminal offence is committed if a person publishes any material which is pornographic, excessively violent or which comes under the provisions of the Obscene Publications Act 1959. Similarly the Protection of Children Act 1978 makes it an offence to publish or distribute obscene material of a child.
- c. **Defamation.** As a form of publication, the Internet is within the scope of legislation relating to libel where a statement or opinion is published which adversely affects the reputation of a person, group of people or an organisation. Legal responsibility for the transmission of any defamatory, obscene or rude remarks which discredit an identifiable individual or organisation will rest mainly with the sender of the email and may lead to substantial financial penalties being imposed.
- d. **Data Protection.** Processing information (including photographs) which contains personal data about individuals, requires the express written consent of those individuals. Any use of personal data beyond that registered with the Data Protection Commissioner will be illegal.
- e. **Discrimination.** Any material disseminated which is discriminatory or encourages discrimination may be unlawful under the Sex Discrimination Act 1975, the Race Relations Act 1976 or the Disability Discrimination Act 1995 where it involves discrimination on the grounds of sex, race or disability.

The above is only designed to be a brief outline of some of the legal consequences of misuse of email facilities.

## Advice on Acceptable and Appropriate Use of Email Facilities

It should be remembered that use of school IT facilities for email in an unacceptable and inappropriate manner and breach of this Procedure may be treated as a disciplinary offence. If users are in any doubt about what constitutes acceptable and appropriate use of email facilities, they should seek the advice and guidance, in the case of members of staff, of the IT Manager, and in the case of students, of their Group Tutor.

## Investigation of Complaints

The school will investigate complaints received from both internal and external sources, about any unacceptable use of email that involves school IT facilities.

The investigation of facts of a technical nature, e.g. to determine the source of an offending email message, will be undertaken by the IT Manager in conjunction with other departments and line managers as appropriate.



Where there is evidence of a criminal offence, the issue will be reported to the police for them to take appropriate action. The school will co-operate with the police and other appropriate external agencies in the investigation of alleged offences.

In the event that the investigation of the complaint establishes that there has been a breach of the standards of acceptable use, then action will be taken as described in Section 8 of this Procedure.



## Appendix E Passwords Procedures

### Purpose

This procedure is to define network passwords and their use.

### Background

- a. Information stored on the computer desktop and the LAN (local area network) forms a part of the school's valuable assets. Strong passwords promote a secure computing environment.
- b. To counter the forces of social engineering (this happens when an attacker tricks users into divulging passwords.) and brute force (these are attempts to gain unauthorised access to systems by trying every combination of letters and numbers until a match is found that allow access) methods of attack, we must be diligent in guarding access to our resources from internal and external threats by adopting strong passwords.
- c. Passwords are the primary authentication method for the school's IT resources and are currently the basic authentication method employed. Passwords ensure that only authorised individuals have access to specific computer systems and establish accountability for all changes made to system resources. Badly chosen passwords endanger the information that they are supposed to protect.
- d. The school needs to institute a robust password procedure if it is to move towards a single-sign-on environment. With a single-sign-on system, a user will be required to authenticate once to gain access to all network resources.

### Scope.

This procedure applies to all staff and students, and any external contractors who are given computer accounts to access information systems owned by or operated by Harris Middle School.

### Responsibility

The staff in the IT Department are responsible for the day to day operation of this procedure. Overall responsibility is with the IT Manager.

### Applicable to:

All Staff and Students.

### Description

- a. Best practices.
  - 1) Passwords should not be written down, emailed or spoken.
  - 2) Passwords must be kept confidential and not shared with colleagues. This does not apply to generic departmental passwords, where a group manages the password.
  - 3) Your username or variations of the username should not be embedded in your password.
  - 4) Passwords must not be blank.
  - 5) Passwords should not be typed or saved in electronic documents.



- 6) Computer generated passwords must be changed following initial successful login.
- 7) Passwords must not be based on personal information (e.g. names of families, pets, name of your street, car registration numbers, telephone numbers)
- 8) Passwords must not be revealed to your line manager.
- 9) Passwords must not be revealed to anyone over the phone.
- 10) Passwords used within the school must not be used for external Internet accounts or online service providers.
- 11) Passwords must not be included in any automated login process.
- 12) Once the passwords have been changed, the new password must be kept for 8 days before the user can be allowed to change it again.
- 13) Passwords must be unique from previous passwords. The previous passwords should not be re-used.

## Password Composition

- i. Passwords must meet the following criteria:
  1. Passwords must be at least eight characters long.
  2. Passwords must be composed of alphanumeric characters (alphabets – A..Z, a..z and numbers – base 10 digits – 0..9).
  3. Passwords should include non-alphanumeric or special characters (e.g. !; £; \$; ); (; %; &; \*; #; @; ?; {; }; [; ]; =; +; >; <; “;”).
- b. Passwords must be strong.
  - ii. Here are some methods for making strong passwords:
    1. You can choose one or two lines from a poem or song and use the first letter of each word. For example ‘Always look on the bright side of life’ becomes alotbsol
    2. Passwords are case sensitive: using the above example, the passwords alotbsol, Alotbsol and aLotBsol are different and the security of passwords can be increased if mixed case passwords are used.
    3. One strategy for creating strong passwords is to replace letters with numbers or characters. For example Alotbsol becomes A10tbs01 where the letter “l” has been replaced with the digit “1” and the letter “o” has been replaced with the digit ‘0’.
- c. Changing your password
  1. Passwords must be changed under any one of the following circumstances:
  2. At least every half term.



3. Immediately, if a password has been compromised or after you suspect that a password has been compromised.
4. Passwords must be changed on direction from the IT Department.
5. Note: You should not change your password last thing on Friday or just before you go on holiday as you may forget it when you need to use it.

d. Good practice/handling

1. A number of shared local administrative passwords may be used on machines for specific departments and computer labs.
2. Passwords must be at least eight characters long but preferably longer.
3. Passwords must be retired after three months.
4. Once the passwords have been changed, the new password must be kept for 8 days before the user can be allowed to change it again.
5. Service accounts must not rely on admin accounts/passwords.
6. Accounts created for external contractors should be given restrictive rights to carry out their functions and the accounts should be disabled immediately following the completion of the appointed task.
7. Administrator/privilege passwords must not be disclosed to external contractors.
8. Default passwords that come with computer systems or services must be changed during installation or immediately after installation.
9. Passwords must be unique from all previous passwords. The last ten passwords must not be re-used.
10. All systems must wherever possible be set up to prompt the user to change passwords in fifteen days.
11. Critical systems must implement account lockout policies and be set up to disconnect idle sessions after a period of inactivity of thirty minutes.
12. Systems must be configured to enforce password changes.
13. The SNMP community strings must be changed from the standards defaults and should be different from the password used to interactively log in.

Privileged passwords should not be communicated via telephone fax or email.



## Appendix F Downloads Procedure

### Purpose

This procedure has been established to set guidelines in an effort to clarify the type and nature of files that employees are allowed to download from third-party sources onto their local computers (desktops, laptops, Pocket PCs, Tablet PCs).

### Applicable to:

All staff.

### Definitions

A download is any file or program that can either be run from or installed to a computer.

### Guidelines

Although it would be impossible to name every executable or download file in this procedure, users should adhere to these guidelines:

- a. The download enhances the employee's productivity.
- b. The download is from a reputable source.
- c. The file does not subject the college to potential liability.
- d. The application, tool, or template has been approved by the IT Network Manager.

### Approved Downloads.

The following is a list of files that employees can download onto their local machines.

#### a. RealOne Player

Employees can use this application to listen to music and view streaming media at their workstation. Users will take care not to adversely affect other workers and will, for example, keep the volume of the music and other media played on this application within reasonable levels, if they are located in an office.

#### b. Adobe Acrobat Reader, Adobe Reader

Users must have this downloaded to view PDF files.

#### c. Internet Explorer Plug-ins

Employees can download plug-ins for use within Internet Explorer, the plug-ins that are currently authorized are;

- Adobe Acrobat plug-in, used for viewing online PDF files
- Adobe Shockwave Plug-in, used for viewing online animated content
- Adobe Flash plug-in, used for viewing online animated content

### Prohibited downloads

The following downloads are not allowed on college computer resources.

#### a. Kazaa Media Desktop

Peer-to-peer file-sharing applications have come under scrutiny in recent years for their ability to allow users to share copyrighted material and for the network resources that they consume.



- b. **WinMX**  
Use of this P2P file-sharing program is prohibited.
- c. **LimeWire**  
Use of this P2P file-sharing program is prohibited
- d. **All other Peer to Peer file sharing programs**  
Use of this P2P file-sharing program is prohibited
- e. **Personal Firewalls**  
While security is an issue that every employee can help manage, the IT Department does not allow the use of personal firewalls on Harris Middle School equipment.
- f. **Any third-party screen saver**  
The use of third party screen savers is prohibited as they are a downloaded file and have to be installed. Unauthorized screen savers can contain viruses and malware causing damage to the network infrastructure and therefore is a prohibited download. Employees will use the default screen savers available on their local machines.
- g. **Non Educational Games**  
Because games provide no benefit to our organization and have a tendency to affect productivity, they are not allowed on school machines.
- h. **Yahoo Desktop & Internet Explorer Toolbar**  
Whilst this program appear to assist the users experience on the internet, this program uses up valuable system resources and can slow a computer down and even cause problems when accessing the internet, therefore this program is not allowed on school computers.
- i. **Google Internet Explorer Toolbar**  
Whilst this program appear to assist the users experience on the internet, this program uses up valuable system resources and can slow a computer down and even cause problems when accessing the internet, therefore this program is not allowed on school computers.
- j. **3M Post-It Notes**  
This program has been known to cause problems with user desktops, therefore it is not allowed on school computers.
- k. **WinZip**  
Whilst this program is a useful tool, it is classed as shareware and continued use over the 40day trial period is against the licence agreement and is in breach of copyright. This program is not required as all functions of this program are built into Windows XP.
- l. **Other**  
Any other program that is available for download that is not specifically in the approved downloads section.



## Appendix G Data Retention Procedure

### Purpose

This procedure is to ensure that members of staff have the information to correctly store and dispose of data within current guidelines.

### Applicable to:

All Academic and Associate staff.

### Definitions

Information includes anything which is recorded in **any** possible form, including handwritten, electronic, audio and video records which are maintained by school staff or their agents.

### Authorisation for Disposal of Information

If there is any doubt about authorisation in specific cases then the IT Manager should be consulted. Disposal guidelines (some of which are legal requirements) for certain types of information are given in the table below. Further guidance on information retention is available on the Joint Information Systems Committee (JISC) website ([www.jisc.ac.uk](http://www.jisc.ac.uk))

### Disposal Procedure for Personal Information on Staff or Students

Minimum retention times for personal information can be found in the school's Data Protection Policy, which has been approved by the Governors. If there is any doubt when deciding retention times not included in the table below, consider the following in order:

- a. Any legal requirements (e.g. litigation is possible up to 6 years after an event).
- b. Length of appeals procedure relating to information.
- c. If the information has not been used during the last 3 years then get rid of it!

Information	Retention Time (years)	Origin / Reason
Student Personal Information: <ul style="list-style-type: none"> <li>• Name and address</li> <li>• Academic achievements, inc. coursework marks</li> <li>• Copies of any references</li> <li>• Other personal data (e.g. health, race, personal matters)</li> </ul>	6 6 5 5	AoC guidance; Limitation period for litigation on negligence is 6 years
Student NVQ Records: <ul style="list-style-type: none"> <li>• Lists of all candidates registered with awarding body for each qualification (inc. name, DoB, address, workplace address, assessor(s) name, IV(s) name, date of registration with awarding body)</li> <li>• Candidate assessment records detailing who assessed what and when, assessment decisions, assessment methods used for each unit/component, location of supporting evidence</li> <li>• Records of IV activity detailing who verified what and when, sample selected and its rationale, records of IV standardisation meetings, assessor and verifier competence records, records of progress towards relevant assessor and verifier awards</li> </ul>	3 years after completion of course	QCA/NVQ Code of Practice



<ul style="list-style-type: none"> <li>• Requirements for the retention of candidate evidence</li> <li>• Records of certificates claimed (inc. unit certificates) and who claimed and when</li> <li>•</li> </ul>		
<p>General Statistical Data on Students</p>	<p>6 years</p>	<p>School guidance; relates to the equivalent of 2 external inspection cycles</p>
<p>Staff Personal Information:</p> <ul style="list-style-type: none"> <li>• Information relating to income tax and NI returns</li> <li>• Information relating to disputes/litigation regarding employment</li> <li>• Personnel files including training records</li> <li>• Staff application forms/interview notes</li> <li>• Facts relating to less than 20 redundancies</li> <li>• Facts relating to 20 or more redundancies</li> <li>• Statutory Maternity Pay records and calculations</li> <li>• Statutory Sick Pay records and calculations</li> <li>•</li> <li>• Wages and salary records</li> <li>• Health records</li> <li>• Health records where reason for termination of employment is connected with health, including stress-related illness</li> </ul>	<p>3 years after end of financial year to which records relate</p> <p>6 Years</p> <p>6 years from end of employment</p> <p>6 months after interview</p> <p>3 years from date of redundancy</p> <p>12 years from date of Redundancy</p> <p>3 years after end of financial year to which records relate</p> <p>As above</p> <p>6</p> <p>During employment</p> <p>3</p>	<p>Employment Tax (employment) Regulations 1993</p> <p>Time limit on litigation</p> <p>References and time limit on litigation</p> <p>Time limit on litigation</p> <p>As above</p> <p>Limitation Act 1980</p> <p>Statutory Maternity Pay (General) Regulations 1986</p> <p>Statutory Sick Pay (General) Regulations 1982</p> <p>Taxes Management Act 1970</p> <p>Management of Health and Safety at Work</p> <p>Regulations Limitation for personal injury claims</p> <p>COSSH Regulations</p>



<ul style="list-style-type: none"> <li>Medical records kept by reason of the Control of Substances Hazardous to Health Regulations 1999</li> </ul>	40	1999
Accident books; records and reports of injuries and diseases	3 years after the date of last entry	Social Security (Claims and Payments) Regulations 1979; RIDDOR 1995
Financial Information: <ul style="list-style-type: none"> <li>European Social Funds</li> <li>Other (invoices, credit notes, etc.)</li> </ul>	12 7	Legal Legal



## Appendix H Incidents Involving Illegal Materials or Activities

### PURPOSE

This procedure is to ensure that members of staff have the information to correctly respond to incidents involving illegal materials or activities.

### BACKGROUND

In the school context, very serious incidents tend to involve illegal materials (particularly the viewing, possession, making and distribution of indecent images of children) or serious stalking or harassment facilitated by communication technologies. Such criminal offences may be committed by pupils and staff alike.

### DEFINITIONS

- Indecent images of children are defined under Section 7 of the Protection of Children Act 1978 (as amended by Section 84 of the Criminal Justice and Public Order Act 1994). References to indecent photographs under the Act include data stored on a computer disk or by other electronic means that is capable of conversion into a photograph.
- The Protection from Harassment Act 1997 is intended to prevent 'stalking' and other similar unsocial conduct. It states that a person must not pursue a course of conduct which amounts to harassment of another, and which he/she knows, or ought to know, amounts to harassment of the other. Although the term is deliberately not defined in the Act, words such as 'alarm', 'distress' or 'torment' fit the term most accurately, and some adverse impact on the victim is required. To constitute a 'course of conduct', harassment must take place on a minimum of two occasions.

### DISCOVERY PROCEDURE

1. If an incident involving illegal materials or activities is suspected initially refer to the flowchart at the end of this document:
  - Discovery of suspected indecent or illegal material within the school's network or premises is a very serious situation, and must always be reported to the police.
2. When an incident is suspected the IT Manager is to initially take control of the situation.
3. It is important that the material is not downloaded, printed or sent by email, because doing so will be an offence in itself.
4. If at all possible, do absolutely nothing to the suspect computer or computers, including turning them on or off. It may be necessary to shut down the whole network, but do not do this unless instructed by the police.
5. Ensure that everyone is kept away and that nothing is touched.
6. Under no circumstances should staff attempt to conduct an investigation of their own, or bring in an outside 'expert' to do so, as this may compromise the evidence if a legal case were to result. In some cases this may constitute a criminal offence in itself.



7. In cases of pupil or staff involvement with indecent materials, it would be advisable for the school to seek legal advice as soon as possible, particularly with regard to the disciplinary actions that are acceptable while the police carry out their investigations.
8. The school should also be prepared for media contact, and have strategies in place for dealing with this.

## **POST DISCOVERY**

In the event of a very serious incident occurring within the school, it is essential that a review of all internet safety policies and procedures is conducted as soon as possible. The Principal would have ultimate responsibility for the review process.

The three key components of a safe ICT learning environment (the infrastructure of whole-school awareness, designated responsibilities, policies and procedures; the effective range of technological tools; and a comprehensive internet safety education programme) should also be reviewed, ensuring that:

- comprehensive debriefing occurs after the incident to maximise what can be learnt;
- the network manager has the professional skills to carry out regular safety checks, and knows the correct protocols to follow if illegal material is suspected or encountered;
- all school staff understand the circumstances under which a forensic audit of computers should be carried out, and by whom, and the appropriate strategies to adopt to ensure that evidence is secured and preserved;
- the school's internet safety team (both policy and management) contains staff with all the relevant expertise, and that the appropriate time and authority is allocated to the team to allow them to carry out their duties effectively.

## **FURTHER INFORMATION**

Further information on illegal content – including when, where and how to report it – can also be found on the Internet Watch Foundation website [<http://www.iwf.org.uk>].



## Appendix I Current Legislation considered for policy formation

### **Computer Misuse Act 1990**

This Act makes it an offence:

- To erase or amend data or programs without authority.
- To obtain unauthorised access to a computer.
- To "eavesdrop" on a computer.
- To make unauthorised use of computer time or facilities.
- To maliciously corrupt or erase data or programs.
- To deny access to authorised users.

### **Copyright, Designs and Patents Act 1988**

This Act, together with a number of Statutory Instruments that have amended and extended it, controls copyright law. It makes it an offence to copy all, or a substantial part, which can be a quite small portion, of a copyright work.

There are, however, certain limited user permissions, such as fair dealing, which means under certain circumstances permission is not needed to copy small amounts for research or private study.

The Act also provides for Moral Rights, whereby authors can sue if their name is not included in a work they wrote, or if the work has been amended in such a way to impugn their reputation.

Copyright covers materials in print and electronic form, and includes words, images, sound, moving images, TV broadcasts and many other media.

### **Crime & Disorder Act 1998**

The Crime and Disorder Act provides the requirement for partnerships between the police, probation, local authorities, health authorities and other agencies. This includes locally targeted and data based strategies that are agreed with the communities.

It is important to note that the Crime and Disorder Act 1998, for the first time placed the coordination of community safety and crime prevention on a statutory basis. Section 5 of the Act makes local authorities and chief police officers the 'responsible authorities' for setting and implementing strategies aimed at achieving reductions in crime.

### **Data Protection Acts 1984 and 1998**

The 1984 Act requires that any person or organisation processing information about individuals in machine-readable form must register with the Data Protection Registrar and must abide by a number of principles.

It also gives individuals the right to inspect information held about them, to demand amendments to records if they are inaccurate, and to sue if they suffer financial damage as a result of incorrect information.



When the 1998 Act was brought fully into force in 2000 it replaced the 1984 Act. It will extend the provisions to material in manual form, and place the onus in many cases on the person or organisation handling the personal information to request permission from the individuals before using the information.

## **Privacy and Electronic Communications (EC Directive) Regulations 2003**

This new directive extends controls on unsolicited direct marketing to all forms of electronic communications including unsolicited commercial e-mail (UCE or Spam) and SMS to mobile telephones; UCE and SMS will be subject to a prior consent requirement, so the receiver is required to agree to it in advance, except in the context of an existing customer relationship, where companies may continue to email or SMS to market their own similar products on an 'opt-out' basis;

## **Protection from Harassment Act 1997**

An Act to make provision for protecting persons from harassment and similar conduct:

1. A person must not pursue a course of conduct—
    - a. which amounts to harassment of another, and
    - b. which he knows or ought to know amounts to harassment of the other.
  2. For the purposes of this section, the person whose course of conduct is in question ought to know that it amounts to harassment of another if a reasonable person in possession of the same information would think the course of conduct amounted to harassment of the other.
  3. Subsection (1) does not apply to a course of conduct if the person who pursued it shows—
    - a. that it was pursued for the purpose of preventing or detecting crime,
    - b. that it was pursued under any enactment or rule of law or to comply with any condition or requirement imposed by any person under any enactment, or
    - c. that in the particular circumstances the pursuit of the course of conduct was reasonable.
- Protection from Harassment Act 1997

## **Protection of Children Act 1976, as amended by Sect 84 of the Criminal Justice and Public Order Act 1994**

### **Children Act 1989 and 2004**

### **Malicious Communications Act 1988**

This includes harassment, bullying, and cyber-stalking

### **Sexual Offences Act 2003**

This includes grooming

### **The Obscene Publications Act 1959 and 1964**

This includes illegal material on, or transmitted via, the web and electronic communications

### **The Telecommunications Act 1984**

This includes illegal material on, or transmitted via, the web and electronic communications



## INCIDENT FLOWCHART

Flowchart for responding to internet safety incidents in school

