



Horbury School
A Specialist Language College

**INFORMATION
TECHNOLOGY
& EMAIL
USAGE
POLICY**

Horbury School

Information Technology Usage Policy

Contents

| | |
|--|----|
| Introduction..... | 3 |
| Installation of software on PC's and Laptops by all users..... | 3 |
| Software Installation by Teachers..... | 4 |
| Treatment of School Equipment by Staff..... | 4 |
| Treatment of School Equipment by Students..... | 5 |
| Network Usage by all Users..... | 5 |
| Data Formats | 6 |
| Acceptable Data..... | 6 |
| Unacceptable Data Formats..... | 7 |
| Internet Usage..... | 8 |
| E-mail Usage..... | 9 |
| Information Security..... | 11 |
| Fault Reporting..... | 11 |
| Complaints..... | 11 |
| Service Levels..... | 11 |

Introduction

This document is meant to give users of the Information Technology (IT) resources provided by Horbury School a set of guidelines and policies for acceptable usage of the equipment and rooms provided. This document will cover the following areas:

1. Installation of software on PC's and Laptops by all users
2. Treatment of equipment by all users
3. Network usage
4. E-Mail usage by all users
5. Internet usage by all users
6. Fault reporting
7. Grievance procedure

It will set out what users are required to accept before they can use the Information Technology facilities at Horbury School and what users can expect from Horbury School when using the IT resources.

These policies are put into place to ensure Horbury School is insulated from the consequences of individual or group actions intent on causing physical damage to IT resources or damage to reputations of individual's being taught, teaching or working at Horbury School. Also they are put into place to prevent the same individual's or groups damaging external organisations in a similar manner through electronic means.

These rules will apply to both staff and students at Horbury School, IT facilities are provided to enable students to learn the given subject being taught and provide some means to save and retrieve work created in the progression of the relevant subject. IT facilities are provided for staff for the development of teaching materials for their students and subject areas and enable staff to perform the administrative duties required by their position.

Situations which are not covered by these statements will be clarified to the best of this documents ability so both staff and students can follow a procedure that is defined as clearly as possible within the changing IT and Government policy environments.

Installation of software on PC's and Laptops by all users

As only certain members of the Horbury School staff have rights to modify a machines configuration, the following rules are applied to software installations to minimise the time spent rebuilding PC's or Laptops which develop problems as a result of unauthorised software installation.

Software Installation by Teachers

1. In general, teachers have the ability to install software on teacher laptops. This should be limited to educational software purely for trial reasons. Should software be of interest for departmental purchase, then the IT department must be notified **in advance** of making the purchase, in order to ascertain its suitability for network use.
2. Other suitable software options, possibly free, should be investigated prior to making any purchase from departmental budgets.
3. Making software ready for network use can take up to a week, if it is possible at all. Software installs are often difficult – allow reasonable time.
4. Do not install any software from internet downloads, always request a CD-ROM from the manufacturer with specific install procedures for an RM network. Downloads may be infected with viruses and other malicious code which could seriously damage network functionality.
5. Do not install software from magazine cover CD's, these applications disclaim any liability for damage and are often pre-production versions with bugs.
6. If in doubt ask IT Support for guidance.
7. Any support calls arising from instances of software malpractice will be referred to heads of department.
8. Any software installed must be for academic purposes, aimed at enhancing Teaching and Learning; software for personal use is not permitted, particularly Instant Messaging or music based applications such as iTunes, however, exceptions may be made if valid reasons are put to the Network Manager.
9. The podium desktop machines are locked down to a greater degree than teacher laptops. Under no circumstances should unauthorised software be installed on these computers. Refer to the network manager.

Treatment of School Equipment by Staff

The equipment is provided to assist staff in achieving their departments and Horbury School's commitments to teaching its students and enabling staff to deliver this in the class room. Changing configuration settings, installing applications or drivers, using the equipment for personal details, personal data storage or use is not approved by Horbury School.

Equipment provided to staff is a loan; as a result, staff taking equipment on loan will be responsible for it. This means that they must be willing to provide sufficient security and respectful treatment of the equipment in question.

A commonsense approach to the equipment is essential, such as not leaving loaded equipment on car seats, parcel shelves etc in plain view when parking in public (and also where staff would normally park their transport). Strong vibration and electrical sources can damage components in most ICT equipment so should be avoided where possible, such as main junction boxes and leaving equipment out of carrying cases or bags when transporting them around.

Loss of components by staff whilst equipment is on loan will result in the cost of replacing the lost component or components' being recharged to the member of staff's

department and the item replacement not being issued again until the recharge is settled. Horbury School expects staff to treat the loaned equipment with care and respect that would be expected of any individual borrowing any item from an organisation in order to perform their duties. If neglect is found to be the cause of any loss or failure of loaned equipment then until the matter is resolved future equipment loans will be declined.

Additionally, data carried on pen drives, external USB disks, handheld devices or laptops must not contain information that could provide personal details of any student. Data protection and child protection protocols are of the highest order. Disciplinary procedures will be taken if sensitive data is taken off site.

Teachers running lessons in IT suites are responsible for maintaining good practice and student discipline during the session. Due diligence is expected and under no circumstances should the class be left alone. This is to avoid unnecessary damage and potentially hazardous interference with cables.

Treatment of School Equipment by Students

Equipment is provided to students to enable them to have an interactive learning environment which provides learning materials through teacher based tutorials and also use of internet information sources.

The student is required to treat this equipment with respect and use in the manner taught by the staff member responsible for the tutorial or tutorials which the student attends. This means no attempts to dismantle, deface interior or exterior components or cases and insert inappropriate materials into media slots if available on the equipment. Removing or interchanging cables or peripheral devices on machines adjacent to each other or around the Horbury School ICT Rooms. Changing the configuration in any way of the equipment provided is not permitted by Horbury School students under any circumstances. Doing so will result in the students ICT access being reviewed. Under no circumstances should any files be brought into the school which could infect or damage the network either by accident or by design.

Bringing USB pen drives or other media into school containing executable files could potentially damage the function of the network. Serious sanctions will ensue with the potential of users being permanently removed from the network if harmful files such as hacking tools are found.

Network Usage by all Users

Horbury School will attempt to provide a means for all users to store data relevant to their position in the school, so they can fulfil the requirements of their teaching or learning needs. As a result this requirement space or data storage will be available to all users, apportioned as best as possible based on:

1. Students course needs
2. Curriculum needs
3. Available space on the network hardware

Data Formats

Acceptable Data

As a result of these criteria, limited space is available to each user, the main limitation being the actual space available on the network hardware. This means Horbury School requires all users only store data or information relevant to curriculum needs on the network, this being images, sounds or text based information relating to course's being taught by staff and studied by students.

Unacceptable Data

Data that will be deemed unacceptable are as follows:

1. **Political**, content presented by minority groups or main stream groups that advocated discrimination or isolation of other groups by its members or affiliates.
2. **Criminal**, content that depicts acts or behaviour that is outside standards of acceptable behaviour defined in law at the time.
3. **Religious**, content that contains icons, teachings, representatives or beliefs of minority or majority groups, which incite violence, mistrust or discrimination by individuals or groups against other minority or majority groups.
4. **Pornographic**, content includes sexual reference's or acts, individual or group, masochistic, sadistic, submissive or domination, fetish, heterosexual, lesbian, homosexual, voyeuristic or paedophilic.
5. **Social**, content referring to individual or group life style choices which could offend those referred to or incites violence or encourages discrimination of those choosing a particular life style choice.
6. **Cultural**, content referring to or quoting a particular individual or groups beliefs, traditions, practices or faiths in a manner that could incite violence or encourage discrimination against those individuals or groups.
7. **Personal**, content not directly related to staff work areas or courses at Horbury School or used to produce course work that is to be assessed.

Unacceptable Data Formats

Currently these are the prominent storage formats. As technology develops new formats will develop if they are not mentioned here it does not mean they are excluded, it only means they haven't been mentioned.

1. **Images** that contain graphic representations moving or still frames or files containing copy righted material whether compressed or uncompressed that require royalties to be paid to the producer or artist. This includes copies of files that the individual owns whether these are Political, Criminal, Religious, Pornographic, Social, Cultural or Personal.
2. **Sounds** containing obscene, abusive, derogatory and biased or incitements to violence against other organisations or individuals, their property, families,

business's and or associates. Files containing copy righted material whether compressed or uncompressed that requires royalties to be paid to the producer or artist, this includes copies of files that the individual owns whether these are Political, Criminal, Religious, Pornographic, Social, Cultural or Personal.

3. **Text** based files that contain statements which will cause offence, incite violence, contain sexual reference or descriptions, advocate extremist or fundamentalist ideologies or encourage illegal activity, files containing copy righted material whether compressed or uncompressed that requires royalties to be paid to the producer or artist, this includes copies of files that the individual owns whether these are Political, Criminal, Religious, Pornographic, Social, Cultural or Personal.
4. **Games** files downloaded from the Internet or brought in on media are not allowed under any circumstances unless they are approved by teachers for teaching purposes. Games for entertainment are non-educational and users found using these files may have Internet access removed.

Space on the network is limited so data that Horbury School finds on the network that is considered to be unauthorised will be removed. Backing up of data will be performed daily; this is another reason for controlling the amount and type of data that is stored on the network. The more data the longer data backups will take, increasing the risk of failure.

Internet Usage

All users of Horbury School's network ICT facilities will ensure that when using the internet applications must agree to visit or browse web sites that are appropriate to the curriculum or subject being taught.

Sites which have content that falls within the unacceptable data criteria must not be visited, browsed or propagated or stored by any methods on the Horbury School network infrastructure. Users must agree not to download data deemed unacceptable as described in the unacceptable data section. Users must agree not to download applications, utilities or program that are pirated, can be used maliciously against Horbury School or other ICT organisations or require a licence agreement.

Do not download and store on the Horbury School network MP3's, WAV, WMA or other audio file formats for personal use. If these files are needed they must be burned onto CD and copied from the CD to the network then removed once finished with.

The school has a responsibility to protect all network users from harmful Internet content and malicious software/viruses by agreeing to web filtering at YHGfL and also having an additional local proxy filter locally. Any attempt to by-pass these systems so that inappropriate or harmful web content can be accessed will bring severe sanctions and trigger disciplinary procedures. These filters are in place to prevent virus or malware infections from unprofessional, non-governed sites.

The use of social websites such as Bebo and Facebook is prohibited and such sites must NOT be accessed in school during teaching hours, nor should Instant Messaging systems. These are recreational tools with no place for them in an academic setting. Additionally, it is not permitted for teachers to have students as contacts on social networking sites or vice versa.

Unacceptable use of Internet outside school

Students should not use the internet or any sites such as Bebo, Facebook or You Tube to publish defamatory or personal comments about members of staff. If they do so this will be dealt with as a serious matter by the Headteacher, resulting in the sanction of isolation or exclusion. Such use of internet sites is abusive and should also be reported to the police by the member of staff concerned. Staff should not post any video images relating to the school or their work at the school on a public website without first consulting the Headteacher.

Information Security

It is imperative that employees maintain an awareness of the importance of security when using or dealing with any form of electronic communications, and that they always take effective steps to ensure that the security and integrity of the school's ICT systems are protected.

This can be achieved through simple but effective steps, such as:

- Never divulging or sharing passwords.
- Not using obvious passwords which are well known to fellow employees, for example children's names.
- Not writing out passwords and leaving them by a workstation.
- Always locking workstations when away from them (for however short a period).
- Logging off when away from the computer for long periods.
- Ensuring that laptops, pen drives, external USB Hard Drives are securely locked away when not in use.
- Data on USB storage devices is backed up to other media and kept safe on a regular basis.
- Home PCs/laptops have an up to date Anti Virus package installed or better still an Internet Security Suite package. All USB devices should be scanned for malicious files before any usage in school.

Maintaining security helps to prevent unauthorised use and the integrity of the school's ICT systems. It also helps to prevent people using another's password and log on to use those systems in an inappropriate, offensive or criminal way.

E-mail Usage

Principles

- School e-mail accounts may not be used for running any form of personal business other than that of an educational nature or relating to Horbury School
- School e-mail accounts may not be used for excessive personal use
- E-mails may not be sent that are illegal, unethical or of an inappropriate sexual nature or that contain inappropriate or abusive language
- E-mails may not be used for bullying, harassment, abuse or other purposes inconsistent with school ethos and policies. Any such usage will lead to termination of e-mail access and disciplinary action.
- Staff and students must not send or forward excessive or inappropriate 'joke' e-mails or chain e-mails.
- E-mails should never be sent during lesson time by staff, as they are deemed to be teaching at that time, unless they form part of the teaching activity of that lesson

- E-mails should not be sent in lesson time by students other than as part of a piece of research or coursework when they may be requesting information, or for a reason sanctioned by a member of staff

Privacy & Confidentiality

- Horbury School supports a climate of trust and respect and does not ordinarily read, monitor or screen electronic mail. School employees who read, disseminate or otherwise compromise the e mails of other staff without the express direction of the Head teacher or his/her designate are subject to disciplinary action, including dismissal. However, when using RM tutor it may be possible for staff to read a student's e-mail or they may want to check the nature of an e-mail sent during a lesson (see above, under principles).
- The school cannot assure the confidentiality or privacy of e-mail. The school is a public institution and any information, including all e-mail communication may be accessed through the freedom of information act or the force of the law.
- The Head teacher may authorise access to employee or student accounts for situations including but not limited to ;
 - Situations involving the health and safety of people or property
 - Possible violations of school or authority codes of conduct, regulations, or policies
 - Child protection issues
 - Other legal responsibilities or obligations of the school

Good Practice

- E-mail is a non-secure medium. Use school e-mail only for communications that you would be comfortable to see in public records
- Identify yourself clearly and accurately in all electronic communications.
- Always include a 'subject' with any mail you send otherwise the mail may be perceived to be SPAM
- In line with Data protection legislation, respect and maintain the integrity of the original author. Treat e-mails as private and confidential unless the author makes them explicitly available to others i.e. do not forward people's addresses to others
- Take appropriate action to ensure that your e-mail does not disseminate computer viruses or other programmes that may damage or place excessive load on school resources
- Refrain from copying all e-mails to many recipients. Only people who directly need to know the contents of the e mail should be copied in. This will help to reduce the bureaucratic burden on students and employees
- Avoid sending multiple e-mails to any one recipient in one day or over a short period of time, especially if they require action, as this may be deemed to be harassment. However, mailshot e-mails may be sent to a group of people as would have been previously done by paper memo
- Staff and students should regularly read, sort, file and delete e-mails. Students and employees should not allow their mail box to become full

Security

- Ensure that your account is used only by you and your account password is known only to you
- Be careful at public workstations to completely log off after using e mail
- Be extremely cautious in transmitting information about students and other individuals and store any such communications in case they are requested under the freedom of information act

If you have any concerns or queries about the appropriate use of e-mail you should discuss them with the Network Manager or the Head teacher.

Fault Reporting

Horbury School operates a web based fault reporting system which allows logging and tracking of calls. Updates are emailed to the user automatically so the current status of any call is known. Access to this is via our website and the Staff menu, by selecting ICT Helpdesk.

Alternatively calls can be logged by emailing:-

helpdesk@horbury.wakefield.sch.uk

or by use of the internal phone system on ext 2000

Complaints

If a problem arises with the support, a member of staff should take this to their Line Manager who will report this to the Network Manager and the problem will be investigated to see if any service level agreement has been broken.

Service Levels

Service levels will be broken down into five groups:

1. **Level 1** - Class room not working, Horbury School Network not available, server failure, eportal failure, internet or mail service failure or any other effect that prevents a large number of ICT resources from being available to the users. Response time within 5 minutes, resolution assessment and action plan will have the highest priority. Users will be informed with timely updates.
2. **Level 2** - Data loss sufficient to cause a restore from backup if available of large amounts of curriculum data, 5 to 6 PC's not working, group of user's e-mail not working and access to personal data or curriculum area, critical printing fault. Response time within 5 minutes, action plan and resolution within 2 hours; users to be kept informed.

3. **Level 3** - Individual PC's or laptop failure, monitor failure, data loss resulting in restore from backup of a curriculum area folder structure, users home folders, 3 – 4 users not getting e-mail or access to curriculum areas or personal data, non – critical printing fault Response times 2 working days, resolution objective within 4 working days but dependant on spares availability.
4. **Level 4** - Work requests – examples are supply of new equipment, changes to room configuration, testing new devices etc. Time lines dependant on nature of the task but the department will endeavour to complete within 2 weeks
5. **Level 5** - Project based requests – Longer term issues and projects requiring research, planning, testing. Planned time frames agreed and timely updates/meetings held.

The above levels are unlikely to take place all at the same time, but this is however what will be implemented if this does happen, depending on staff availability and existing work load. Work requests will be dealt with as promptly as possible and as they are requested.

Jobs will be prioritised based on their level and degree of immediacy, and will always be dependant on staff availability, existing workload, and spares availability.