# Priestnall School

## IT acceptable use policy

# IT acceptable use policy

## Contents

## 1 Introduction

**1.1** The purpose of this document is to ensure that all users (students, employees, parents, visitors etc.) of Priestnall School ICT Facilities are aware of the policies in place relating to their use.

Effective and proper use of information technology is fundamental to the successful and efficient running of Priestnall School. However, misuse of information technology - in particular misuse of e-mail and access to the Internet - exposes Priestnall School to liability and is a drain on time and money. It is critical that all users read and understand this document and make themselves aware of the risks and exposure involved.

**1.2** It is the responsibility of all users of Priestnall School's ICT Facilities to be aware of and follow all policies and guidelines and to seek advice in case of doubt. Priestnall School's ICT policies are published on the Intranet and on the School website in the Policies section.

**1.3** This policy may be updated or supplemented by specific standards or procedures to reflect further developments in technology or legislation or other relevant changes. Priestnall School reserve the right to amend the policy without prior warning.

**1.4** Priestnall School encourages the use of its ICT Facilities for the mutual benefit of Priestnall School, its students, parents, partners and employees. ICT when used in the proper manner is an extremely valuable tool for all those with a vested interest in pushing Priestnall School forwards, for example it enables students to partake in independent learning. Similarly the regulations that constitute this policy seek to provide for the mutual protection of Priestnall School and the rights of its students and employees.

**1.5** Priestnall School aims to keep the Acceptable Usage Policy as a "live" document, and as such is open to being regularly reviewed. Therefore, Priestnall School reserves the right to make amendments without prior notice. As a result, Priestnall School expects its Staff/Pupils to take responsibility for reading and upholding the standards laid out in the Acceptable Usage Policy.

**1.6** All users should understand that this policy will be consistently enforced.

## 2 ICT Facilities

Access to corporate ICT Facilities is managed by ICT Technical Support. Use of any of Priestnall School's ICT Facilities is at the discretion of Priestnall School.

### 2.1 Definition

The phrase 'ICT Facilities' as used in this policy shall be interpreted as including any computer hardware or software owned or operated by Priestnall School and any allocation of time, memory, disk space or other measure of space on any of Priestnall School's hardware, software or network.

### 2.2 Ownership

ICT Facilities owned by Priestnall School and software and/or data developed or created (for whatever reason) on that equipment remains in all respects the property of Priestnall School. The Patents Act 1977 and the Copyright, Designs and Patents Act 1988 provide for the Intellectual Property Rights (IPR) in that work created by an employee in the course of his/her employment is vested automatically to the employer.

### 2.3 Desktop PCs

Desktop PCs are a critical asset to Priestnall School and must be managed carefully to maintain security, data integrity and efficiency. For clarification of a machine's status as a 'Desktop PC' please consult ICT Technical Support. Non-standard software shall be interpreted as any software that does not comply with the regulation of sub-section 2.5 below.

All users have access to appropriate areas on Priestnall School file servers for the secure storage of valuable files. Valued documents and files should not be stored on Desktop PCs or Laptops. Files stored on Desktop PCs or Laptops are at risk of loss through hardware/software failure or automated administrative activity. For which Priestnall School ICT Technical Support accepts no responsibility.

Desktop PCs are defined as the CPU/hard-drive unit, Monitor, Keyboard and Mouse all of which are asseted components and further, are subject to change control. Users must contact IT Technical Support in order to perform a 'swap' of these assets.

### 2.4 Portable PCs

Portable PCs are at high risk from loss or theft and require additional security protection. All reasonable precautions must be taken to ensure that hardware is stored securely and in line with LEA recommendations. Also, to protect the integrity of Priestnall School systems and data procedures, passwords or authentication devices for gaining remote access to Priestnall School systems must not be stored with the computer. This includes the saving of passwords into remote access software.

Highly confidential data can be encrypted to protect it in the event of Portable PC loss. IT Technical Support can help with this process.

If your Portable PC is lost or stolen IT Technical Support must be notified ***as soon as possible and a report made to the police***.

**No communications device, whether school provided or personally owned, may be used for the bullying or harassment of others in any form.**

**All users have a responsibility to report any known misuse of technology, including the unacceptable behaviour of others.**

**All users should use the network responsibly. Wasting staff effort or network resources, or using the resources in such a way so as to diminish the service for other network users, is unacceptable.**

### 2.5 Technical Safeguards

All users should be aware that Priestnall School has in place, at both council level and school level, a number of technical safeguards designed to protect all users and the Priestnall School ICT Facilities. These safeguards are aimed

at protecting all users from inappropriate material that may be available via the internet and email. In addition, these safeguards aim to protect the Priestnall School network from malicious software and inappropriate files which could be brought on site.

**All users have a duty to respect the technical safeguards which are in place. Any attempt to breach the technical safeguards, conceal network identities or gain unauthorised access to the systems and services is unacceptable.**

**All users have a duty to report failings in technical safeguards which may become apparent when using systems and services.**

**All users should be aware that, Priestnall School reserves the right to monitor network activity and online communications, including any personal or private communications made via the school network.**

### 2.6 Software

Only software properly purchased/licensed and/or approved by ICT Technical Support may be used on Priestnall School hardware. Non-standard or unauthorised software can cause problems with the stability of corporate computing hardware and it is necessary to contact ICT Technical Support for the approval of the installation of such software.

Software or shareware may be downloaded from the Internet or loaded from other sources (e.g. CDROM) onto school provided laptops when necessary, however it is the responsibility of the individual to ensure that any licensing issues are addressed promptly, either by on-line registration or the purchasing of a valid licence through ICT Technical Support.

In order to comply with our registration with the 'Federation Against Software Theft' ICT Technical Support must be notified when such additional/new software is installed. The use or copying of software without the licensor's permission is illegal and equally the terms and conditions of software licences must always be adhered to.

Whilst it is the user's responsibility to take reasonable care over the configuration of their computer hardware, it is possible for software to be installed on a machine without the full comprehension of the user. Users discovering software that has been installed in an unsolicited manner and which contravenes the licensing regulations above are encouraged to contact ICT Technical Support who will be happy to assist in resolving any issues.

### 2.7 Data security

You must only access information held on Priestnall School computer systems if you have been properly authorised to do so and you need the information to carry out your work. Under no circumstances should you disclose personal or other confidential information held on computer to unauthorised persons. The unauthorised access to and/or unauthorised modification of data is a criminal offence under the Computers' Misuse Act 1990.

It is School policy to store data on a network drive where it is regularly backed up. **You** must ensure that data that is not stored on the network file server is regularly backed up (for example, any files stored on the desktop of your laptop are not backed up on the network file server).

### 2.8 Personal data and the Data Protection Act

Priestnall School maintains a notification to the Data Protection Commission in compliance with the Data Protection Act 1998. This notification is held on a public register and contains details of the organisations holding and processing of personal data.

The Network Manager must be informed of all collections of personal data. It is the responsibility of all Priestnall School staff to ensure that personal data is held and processed within the terms of Priestnall School notification and in compliance with the data protection principles.

Personal data shall be:

- obtained and processed fairly and lawfully
- held for specified lawful purpose(s)
- not used or disclosed in a way incompatible with the purpose(s)
- adequate, relevant and not excessive for the purpose(s)
- accurate and up to date

- not kept longer than necessary
- available to the data subject
- kept secure.

Staff should note that all data and correspondence, including e-mail messages, held by Priestnall School may be provided to a data subject, internal or external, in the event of a subject access request.

### 2.9 Freedom of Information Act

Priestnall School is subject to the provisions of the Freedom of Information Act (2000) which provides for the general right of access to information held by public authorities. Users should be aware that the Act effectively extends rights available under the Data Protection Act to include all types of information held, whether personal or non-personal. Therefore, such data or correspondence may be provided to an applicant in the event of an access request.

### 2.10 Virus protection

Anti-virus software is loaded on all computers as standard and is updated regularly via the network.

Anti-virus software must not be de-installed or deactivated. Files received by or sent by e-mail are checked for viruses automatically.

Users must not intentionally access or transmit computer viruses or similar software.

Non-Priestnall School software or data files intended to be run on Priestnall School equipment by external people such as engineers or trainers must be checked for viruses before use. If you suspect that a virus has infected a computer then stop using the computer and contact ICT Technical Support immediately.

### 2.11 Network access

Passwords protect Priestnall School systems from access by unauthorised people: they protect your work and the School's information. Therefore never give your network password to anyone else without the Network Manager's permission.

Procedures are in place on systems to ensure users change passwords on a regular basis, passwords are of a minimum length and old passwords cannot be reused immediately.

Passwords must conform to the ICT Technical Support specification.

Priestnall School does not allow the connection of non-corporate computer equipment to the network without prior written request and technical approval. This includes connection via dialup or Virtual Private Networking (VPN).

### 2.12 Further general guidance

Priestnall School users must ensure prior approval at a Network Manager level to:

- Set-up World Wide Web sites on Priestnall School ICT Facilities
- Publish pages on external World Wide Web sites containing information relating to Priestnall School
- Enter into agreements on behalf of themselves or Priestnall School via a network or electronic system
- Transmit unsolicited commercial or advertising material to other users of a network or to other organisations
- Be used for external business interests or personal gain

## 3 Electronic mail

### 3.1 Use and responsibility

Priestnall School electronic mail (e-mail) system is provided for Priestnall School's authorised purposes. E-mail is now a critical business tool but inappropriate use can expose Priestnall School and the user to significant liability.

Liability can arise in a number of ways including, among others, copyright or trademark infringement, misuse of confidential information, defamation and liability for inaccurate statements.

The e-mail system costs Priestnall School time and money, it must be used judiciously in the same manner as other Priestnall School resources such as telephones and photocopying.

Priestnall School wide e-mail messages must be work related and of significant importance to all employees.

### 3.2 Content

E-mail messages must be treated like any other formal written communication and cannot be considered to be private, secure or temporary.

Email can be copied and forwarded to numerous recipients quickly and easily and you should assume that they could be read by anyone.

Improper statements in e-mail can give rise to personal liability and liability for Priestnall School and can constitute a serious disciplinary matter.

E-mails that embarrass misrepresent or convey an unjust or unfavourable impression of Priestnall School or its affairs, employees, students, or competitors are not permitted. **Do not** create or send e-mail messages that are defamatory.

Defamatory e-mails whether internal or external can constitute a published libel and are actionable.

Never send confidential or sensitive information via e-mail. E-mail messages, however confidential or damaging, may have to be disclosed in court proceedings.

Do not create or send e-mail messages that may be intimidating, hostile or offensive on the basis of sex, race, colour, religion, national origin, sexual orientation or disability.

It is never permissible to subject a student or employee to public humiliation or ridicule; this is equally true via e-mail.

Copyright law applies to e-mail. Do not use e-mail to transmit or circulate copyrighted materials.

### 3.3 Privacy

E-mail messages to or from you cannot be considered to be private or confidential. Although it is not policy to routinely examine the content of individuals e-mail, Priestnall School reserves the right to monitor messages, at any time, for specific instances in which there is good cause for such monitoring or some legal obligation to do so. Good cause shall include the need to fulfil statutory obligations, detect student or employee wrongdoing, protect the rights or property of Priestnall School, protect IT system security or to comply with legal process.

Messages sent or received may be copied and disclosed by Priestnall School for lawful purposes without prior notice.

It is not permissible to access or to send e-mail from another user's personal account either directly or indirectly, unless you obtain that person's prior written approval.

## 4 Internet usage

The laws of all nation states regulating such diverse subjects as intellectual property, fraud, defamation, pornography, insurance, banking, financial services and tax apply equally to on-line activities. However, the practical legal position regarding Internet usage is often uncertain.

Strictly, documents must not be published on the web which are defamatory or which may constitute intimidating, hostile or offensive material on the basis of sex, race, colour, religion, national origin, sexual orientation or disability under the sovereign law of the country in which the web server hosting the published material is sited.

Strictly, material must not be accessed from the web which would be objectionable on the above grounds under the sovereign law of the countries in which the networks transporting the material are sited or which would violate the Acceptable Use Policies of those networks.

Given the impracticality of assessing the exact legal position with regard to the previous two paragraphs, Priestnall School Acceptable Use Policy governing material that could be objectionable on the above grounds is grounded in English law, on which basis it is reasonable to expect Priestnall School staff/pupils to have good awareness and to be able to exercise good judgement. If in doubt over a specific case please discuss with your Line Manager/Teacher.

Once information is published on the worldwide web anyone from anywhere in the world can access it.

It is therefore critical that material of a proprietary or sensitive nature should not be published on unsecured public web sites.

All Internet usage from the Priestnall School network may be monitored and logged for reporting on aggregate usage. When specific circumstances of abuse warrant it, individual web sessions will be investigated and linked to the relevant employees user account. Such an investigation may result in action via the Priestnall School Disciplinary Procedure and possibly criminal investigation.

**All users should understand that Priestnall School reserves the right to monitor network activity and online communications, including any personal or private communications made via the school network.**

**All users should be aware, that in certain circumstances where unacceptable use is suspected, Priestnall School reserve the right to use enhanced monitoring and procedures may come into action, including the power to check and/or confiscate personal technologies such as mobile phones.**

Copyrights and licensing conditions must be observed when downloading software and fixes from the web sites of authorised software suppliers. Files so protected must never be transmitted or redistributed to third parties without the express permission of the copyright owner.

### 4.1 Newsgroups

Postings to newsgroups are in effect e-mails published to the world at large and are subject to the same regulations governing email as above.

Always include a disclaimer with a posting if it could be interpreted as an official statement or policy of Priestnall School. For example:

"The views expressed are my own and do not necessarily represent the views or policy of Priestnall School."

### 4.2 Instant messaging

Instant messaging is free, fast, real-time and powerful. However instant messaging also carries inherent risks: lack of encryption (allowing the possibility of eavesdropping) logging of chat conversations without a user's knowledge and virus risks. Due to these risks, Priestnall School does not currently allow the use of instant messaging for the communication of sensitive or proprietary information.

## 5 Private use, legislation and disciplinary procedures

### 5.1 Private use

ICT Facilities are provided for Priestnall School business purposes and responsible personal use is allowed provided there is no conflict with the interests or requirements of Priestnall School. Priestnall School does not accept liability for any personal loss or damage incurred through using the School ICT Facilities for private use.

### 5.2 Updates to this Policy

In the light of changes in the School, technology, legislation or relevant standards it may be necessary to update this policy from time to time. Notification to all staff will be made when updates are available.

### 5.3 Relevant legislation

The following are a list of Acts that apply to the use of PRIESTNALL SCHOOL ICT Facilities:

- Regulation of Investigatory Powers Act 2000
- Computers' Misuse Act 1990
- Protection from Harassment Act 1997
- Sex Discrimination Act 1975
- Race Relations Act 1976
- Disability Discrimination Act 1995
- Obscene Publications Act 1959
- Telecommunications Act 1984
- Protection of Children Act 1978
- Criminal Justice Act 1988
- Data Protection Act 1998
- The Patents Act 1977
- Copyright, Designs and Patents Act 1988
- Defamation Act 1996
- Freedom of Information Act 2000
- Human Rights Act 1998

### 5.4 Disciplinary and relation action

Priestnall School wishes to promote the highest standards in relation to good practice and security in the use of information technology. Consequently it expects and supports the integrity of its students and employees.

In exceptional circumstances, where there are reasonable grounds to suspect that a student or an employee has committed a serious criminal offence, the police will be informed and a criminal prosecution may follow.

Appendix 1 details examples of behaviours which are unacceptable within Priestnall School and provides examples of behaviour deemed as Gross Misconduct and Misconduct.

Appendix 2 outlines procedures to be followed in cases of suspected abuse of computers that constitute Gross Misconduct.

Appendix 3 outlines procedures to be followed in cases of suspected abuse of computers that constitute Misconduct.

## 6.0 Printing

### 6.1 Use and Responsibility

Priestnall School provides high quality facilities for printing in all areas of the school.

However, like all IT facilities within Priestnall School printing is a privilege which, if abused, can and will be removed from those persons mistreating it.

All printing consumables will be paid for from departmental capitation.

### 6.2 Monitoring

Priestnall School reserves the right to monitor all printing being done on site.

### 6.3 Sanctions

Acceptable use of printing is in conjunction with the guidelines set out in the Priestnall School ICT Acceptable Use Policy.

In the event of an act of Misconduct/Gross Misconduct, the school's disciplinary policy will be administered accordingly (as outlined in Appendix 1-3).

## Appendix 1: Examples of behaviours which require the use of the PRIESTNALL SCHOOL disciplinary policy

**GROSS MISCONDUCT** Examples.

1. Criminal Acts – for example in relation to child pornography.
2. Visiting pornographic sites (adult top shelf materials)
3. Harassment – inappropriate e-mails or printed e-mails sent to a colleague, even if sent as a joke. Harassment can take a number of forms and is defined as unwanted conduct that affects the dignity of people within the workplace.
4. Obscene racist jokes or remarks which have been shared internally and externally – reflects on the image of employer and brings the organisation into disrepute.
5. Downloading and installation of unlicensed products.
6. Viewing sexually explicit materials, except where this forms an authorised part of the employee's job (for example monitoring usage).
7. Chat rooms – sexual discourse, arrangements for sexual activity.
8. Violation of Priestnall School registration with the Federation Against Software Theft – such as software media counterfeiting or illegitimate distribution of copied software.

**MISCONDUCT** Examples.

1. Frivolous use of School ICT Facilities that risk bringing Priestnall School into disrepute. The distribution of animated Christmas card programmes or 'chain e-mails' beyond the internal e-mail system would represent examples of such misconduct.
2. Entering into contracts via the Internet that misrepresents Priestnall School.
3. Contracts are legally binding agreements and an employee must not enter into any agreements via the Internet to procure goods or services where Priestnall School is liable for this contract, without first consulting Priestnall School Financial procedures (available from the Finance Department).
4. Deliberate introduction of viruses to systems.

This list is not exhaustive, but sets the framework of Priestnall School approach to misuse of computing systems.

Priestnall School has the right to monitor employees use of computer equipment where there is evidence to suggest misuse. (Regulation of Investigatory Powers Act 2000).

## Appendix 2: Action to be taken in cases of suspected abuse of computers if gross misconduct is suspected

Where a manager suspects misuse by a *user*;

Contact with Network Manager or Assistant Network Manager to provide data on the individual's use of computer.

The Network Manager or Assistant Network Manager will make a judgement based on information available as to whether investigation is necessary and will discuss evidence with the Senior Member of Staff Responsible.

If yes, the Senior Member of Staff Responsible will:
Discreetly stop the user from using the computer further. Ask the user to attend a private area with a friend or colleague in attendance.

If the user is a student then parents will be notified immediately and the Priestnall School sanctions system implemented.

On the facts that are immediately available, a decision will be taken whether to refer the matter to the Police for criminal investigation. This does not preclude the matter being referred to the Police at any later stage when a formal investigation has been undertaken within the disciplinary procedure.

**Priestnall School Disciplinary Procedure**
The Senior Member of Staff Responsible will then report the issue to the Headteacher who will arrange a formal investigation and the Priestnall School disciplinary Policy will be adhered to where required. The outcome of which may range from detentions, to removal of internet access through to full exclusion if so required.

## Appendix 3: Action to be taken in cases of suspected abuse of computers which does not constitute gross misconduct

Where a user is suspected of misuse:

Contact with Network Manager or Assistant Network Manager to provide data on the individual's use of computer.

The Network Manager or Assistant Network Manager will make a judgement based on information available as to whether investigation is necessary and will discuss evidence with the Senior Member of Staff Responsible.

If yes, the Senior Member of Staff Responsible will:

Investigate by asking the user for an explanation and make other enquiries and investigate as required. If the user is a student then parents will be notified immediately, and the Priestnall School sanctions system implemented.

At the conclusion of the investigation if there are reasonable grounds to conclude that a criminal act has taken place then the procedure for Gross Misconduct will apply.

The Senior Member of Staff Responsible may:

make a judgement that a verbal warning is needed
or make a judgement that a written warning is needed
or remove the use of the facility
or enter the disciplinary process and convene a disciplinary hearing
or decide there is no case to answer and the matter concludes