# Information Acceptable Use Policy

To use this template, simply replace the text in dark grey with information customized to your organization. When complete, delete all introductory or example text and convert all remaining text to black prior to distribution.

|  |  |
| --- | --- |
| **Policy Owner** | Name the person/group responsible for this policy’s management. |
| **Policy Approver(s)** | Name the person/group responsible for implementation approval of this policy. |
| **Related Policies** | Name other related enterprise policies both within or external to this manual. |
| **Related Procedures** | Name other related enterprise procedures both within or external to this manual. |
| **Storage Location** | Describe physical or digital location of copies of this policy. |
| **Effective Date** | List the date that this policy went into effect. |
| **Next Review Date** | List the date that this policy must undergo review and update. |

# Purpose

Describe the factors or circumstances that mandate the existence of the policy. Also state the policy’s basic objectives and what the policy is meant to achieve.

The purpose of this policy is to provide staff with clear guidance on the appropriate, safe, and legal way in which they can make use of information and IT equipment in [Company Name]. Staff need to be aware of the compliance required with this policy and [Company Name’s] commitment to comply with the [specific policy document or regulations that define the requirements for information handling and communication] requirements that all reasonable organizational and technical measures are taken to safeguard its data.

# Scope

Define to whom and to what systems this policy applies. List the employees required to comply, or simply indicate “all” if all must comply. Also indicate any exclusions or exceptions i.e. those people, elements or situations that are not covered by this policy or where special consideration may be made.

This Acceptable Use Policy (AUP) applies to the use of all information and IT equipment by [Company Name] staff (including temporary workers, locums, and staff seconded or contracted from other organizations). All staff should be aware of their legal obligations and internal policy in respect of information handling.

This policy should be a living document that will change as information use changes in the organization.

All employees are expected to have knowledge of at least the portions of this document that are directly related to their role within the organization.

# Definitions

Define any key terms, acronyms or concepts that will be used in the policy. A standard glossary approach is sufficient.

1. **Low Risk Information.** This is defined as information that does not require special protective measures.
2. **High Risk Information.** This is defined as information, the loss or breach of which would substantially impair a company.

# Governing Laws & Regulations

If applicable, list any laws or regulations that govern the policy or with which the policy must comply. Confirm with the legal department that the list is full and accurate. If there are no pertinent governing laws or regulations, delete this section.

# Policy Statements

Describe the rules that comprise the policy. This typically takes the form of a series of short prescriptive and proscriptive statements. Sub-dividing this section into sub-sections may be required depending on the length or complexity of the policy.

1. The primary responsibility for determining changes to the AUP belongs to the [role, position] for [Company Name]. As such, this person is the executive responsible for managing organizational risk. The policies and rules are a direct consequence of the Information Governance charter.
2. The Head of IT is responsible for ensuring any of [Company Name’s] technical systems can meet our risk management needs as defined by compliance rules. All projects that use or require access to information handling systems (ECM, fileshares, CRM, website, ERP, etc.) must be introduced through the IT department.
* The [CIO and the IT department] are responsible for ensuring that the project or device is able to comply with all of the security requirements within this policy. Compliance also requires that staff are aware of their responsibilities so the [CIO and IT] are responsible for ensuring any training needs for IT equipment introduced by the department are met.
1. [Company Name’s] [Information Asset Manager (IAO)/Information Steward] is responsible for ensuring [Company Name] rules and policy on acceptable use of equipment are explained clearly as part of [Company Name’s] induction training for new staff. [The IOA/Information Steward] is also responsible for ensuring the correct processes are followed when breaches of information risks or potential breaches occur, via [Company Name’s] incident reporting procedure.
2. All [Company Name] staff, (including temporary or honorary staff), who have access to and make use of IT equipment and [Company Name] IT systems are responsible for using it in accordance with the rules within this policy. In particular, all staff must ensure that they use systems in such a way that they ensure patient and staff confidentiality is maintained.
3. The [Information Governance Leadership (IGL)] is responsible for overseeing the Information Governance program’s policies and rules. As such it has primary ownership of this policy and final say on any changes to the document.
* Any requests for [IGL] decisions on changes to this policy must be placed through the [IAOs] who have the role of day-to-day implementation of these policies.
* The [IGL] will work with [IT steering committee and the executive board] to determine the project backlog.
1. Staff will be provided with clear guidance and procedures regarding:

* How to use systems properly to ensure that information recorded is correct, up to date, and complete
* How to access help facilities
* Clear, current, and relevant definitions of information required

These procedures shall be available to all staff at the point of data capture and retrieval, and there shall be processes in place to ensure compliance.

1. The effectiveness of this policy will be ensured by way of a [quarterly, annually] review of reports as part of the Information Governance committee’s meeting. It is expected that IT service desk will record any incidents showing non-compliance. A database is maintained by the IT service desk to allow for review of any patterns.
* New members of staff are given a copy of the AUP on recruitment to [Company Name].
* [Company Name]’s established [Information Asset Owners (IAOs)] may also be asked to confirm that this policy is effective within the departments they oversee. Results of audits of local IT systems will be reviewed to ensure that a picture is obtained of the extent to which the Acceptable Use Policy is clearly understood by all staff.
* Local experts and departments are expected to audit their own practices from time to time to measure compliance with this policy or in light of future [Company Name] requirements.
1. Staff will only access IT systems provided to them for duties in connection with their employment or engagement and in accordance with their terms and conditions of employment or equivalent. Access to some applications and information sources will be routinely recorded and/or monitored for this purpose.

* Any changes to information access designed to expand use or change the storage location of information sources requires approval through the [Information Governance committee].
1. [Company Name] systems must not be used for the creation, transmission, or deliberate reception of any images, data, or other material that is designed or likely to cause offence or needless anxiety, or is abusive, sexist, racist, defamatory, obscene, or indecent. When communicating electronically, staff are expected to conduct themselves in an honest, courteous, and professional manner.
2. [Company Name] systems must not be used for private work, or for storage of personal non-work related files, except where prior arrangements have been agreed with [Company Name] (other personal use may be allowed outside working hours with the permission of line managers and with appropriate payment for consumables).
3. Staff may not use [Company Name’s] IT facilities for commercial activities. This includes, but is not limited to, advertising or running any sort of private business.

* Use of the internet facility for commercial activities other than in the conduct of [Company Name] business is prohibited.
* Use of the internet facility for political activities is prohibited.
* Staff may not use [Company Name’s] IT facilities for advertising or fundraising for commercial or charitable organizations not directly connected with [Company Name].
1. It is the responsibility of all staff to ensure that computer systems and facilities and the data, which is accessed through them, are safe and secure. Systems should be placed in an area where it is not likely to be damaged and where the content of screens cannot be read by unauthorized people.

* All staff will ensure that any print-outs or other outputs from [Company Name] systems are appropriately protected and disposed of when no longer needed. Printouts may not be copied, removed from the workplace, or shared with others without proper authorization.
* Any member of staff who suspects or is made aware of a security breach must immediately alert the IT service desk who will initiate investigation procedures. Depending on the breach scenario, investigations will be carried out jointly with [Company Name’s] [Information Governance Manager, IT Security Manager, the Caldicott Guardian, and appropriate senior management]. If warranted, the findings will be subsequently reported to [Company Name] Board and to the Security Incident Reporting Scheme.
1. Deliberate activities with any of the following consequences (or potential consequences) are prohibited:

* Corrupting or destroying other users' data.
* Using systems in a way that denies service to others (e.g. overloading the network).
* Wasting staff effort or computing resources including staff involved in the support of those resources.
* Gaining access to systems that you are not authorized to use.
1. Staff shall ensure that there is a clear, regular process of audit for the quality of information captured, including the use of feedback from external sources and from validation reports. Audit trails should be used to identify where any identified errors have occurred. There shall be a mechanism to rectify any issues and ensure that any consequent training needs are built into refresher training for appropriate individuals.
2. It is permissible for staff to send and receive email at work for incidental personal purposes, provided that this does not involve a substantial expenditure of time, or use for profit.
* Personal email should not add a significant burden to [Company Name] IT systems.
* The size of messages, the frequency with which they are sent, and the number of recipients (within [Company Name]) should not be excessive, and may be monitored to ensure system performance.
* [Company Name] has the final decision on what constitutes excessive use. Staff must act in accordance with their manager’s local guidelines.
* It is not permitted to write or present views on behalf of [Company Name] unless authorized to do so.
1. No personally identifiable information or records should be transmitted via email to any external account, this includes personal accounts of [Company Name] employees. Any need to share this kind of information should be performed using the system features. End users are not to provide records to co-workers who do not have access to the system or are outside of the corporate walls.
* Email queries received from members of the public should always be responded to in writing, not electronically, as it is not possible to be certain that the sender is who they appear to be, or that the message will be read by them.
1. Staff should treat email attachments that have been sent unsolicited with extreme caution, especially if the sender is unknown. Viruses are often sent this way. If staff are not sure what an attachment is for, or why someone has sent it to them, they should not open it, and seek advice from the IT Service Desk.
* To intentionally introduce files that cause computer problems is strictly forbidden and could be prosecutable under the Computer Misuse Act 1990.
1. When sending emails to a distribution list:

* Do not send or forward email to any large group of staff unless there is a genuine reason for them to read it.
* Do not advertise by email.
* Do not circulate warnings about any virus risk, but consult with the IT service desk.
* When sending email to external addresses, consider the possibility that this action may inadvertently reveal email addresses to third parties.
1. Staff should not set up auto-forward rules from their email mailboxes.
2. Forging an email (or any other electronic message), or sending email from any account other than your own without permission may be treated as fraud.
3. Email will not be used for intentional receipt and/or distribution of offensive, obscene, or pornographic material. There is a legal requirement for the Chief Executive to report any computer crime involving child pornography to the police. If staff receive an email connected with child pornography, they should seek advice from their manager immediately so that [Company Name] can take appropriate preventative action.
* If staff receive any pornographic or offensive email, they should not open it or print it. Staff must fill in an incident form and let [IT Security Manager and RUH Risk Manager] know they have received it.
* If staff receive an email containing sexually or racially abusive or discriminatory phrases or material, again they should seek advice from their manager.
* No member of staff is permitted to distribute email that contains offensive material. Offensive material is defined by [Company Name]’s Equal Opportunity and Harassment Policies and includes hostile text or images relating to gender, ethnicity, race, sex, sexual orientation, religious or political convictions and disability. This list is not exhaustive. Other than instances which demand criminal prosecution, [Company Name] is the final arbiter on what is or is not offensive material, or what is or is not permissible use of email.
1. Any computing system owned or provided by [Company Name] is subject to the same conditions of use whether used at home or in the office.

* Users should take all reasonable care and precautions to ensure safe transport and storage when moving equipment between home or other remote locations and work, keeping it locked and out of sight.
* Users may be held fully or partially liable for any loss, damage, or theft occurring to [Company Name] IT equipment whilst in their care. Users are within their rights to refuse to take information and equipment offsite if they feel circumstances mean that they are not able to protect it adequately.
* All [Company Name] confidential documentation, whether in paper or data format, should be stored in a secure area of users’ homes or the remote location they are working from.
* For further guidance, staff should refer to the [mobile information handling and computing policy].
1. The use of any customer- or HR-related identifiable information on staff-owned equipment is strictly forbidden without the authorization of the department’s [Information Asset Officer].

* [Company Name] business information (such as spreadsheets, plans, and reports etc.) may be used, but not be stored permanently on staff-owned equipment or user-acquired applications.
* To restrict the possibility of viruses being transmitted to the organizational computers and network, staff must not use their own computer for work-related activities unless anti-virus software and a firewall have been installed and are regularly updated.
* Personal mobile devices may be synchronized with work email for calendar, contact, and email purposes where permitted by email policies and guidance.
* In circumstances where the organizational resources do not meet the needs of end users, project or access requests can be submitted through normal IT channels.
1. On request, the IT department will provide each member of staff with a personal username/password or “smartcard.” These must be used to gain access to any [Company Name] computer. Usernames/passwords and smartcards will only be issued when authorized by an appropriate authorized signatory, and when identity checks have been completed satisfactorily.

* Before a password/smartcard is issued, staff must complete the appropriate authorization/registration forms that will request the user to read, understand, and abide by the terms of this overarching Acceptable Use Policy.
1. The IT department will endeavor to provide all systems with secure access facilities. Access to databases or systems containing important, sensitive, and/or confidential information will be restricted to those staff who require access as part of their job function. These may be protected by additional security controls.

* Where passwords are used, users will be able to select and change their own password by using a minimum of 8 characters (number and letters). The only exceptions to this are where the security controls on older computers are not available or system configuration passwords are not tied to a particular user.
* Users should not leave any computer unattended without either logging out or activating a password-protected screensaver. Where a previous user has left their access open, new users must log out from that session first.
* Users should not add additional password or security measures to any computer or files without first consulting with the IT department.
* Attempting to remove or bypass any security access on any [Company Name] computers is strictly forbidden.
* Passwords are issued for personal use only. They should not be shared or disclosed to anyone else. Users are required to protect their usage against loss, damage, or theft and against possible misuse by others. If a breach of security is recorded, the burden of proof will be with the registered user to show that they are not responsible for the breach.
* Users should report any known or suspected breaches of information security to the [Information Governance Manager] or IT service desk for any necessary action to be considered and undertaken.
1. All staff are responsible for ensuring that confidential information is stored securely and that appropriate confidentiality is maintained when handling information.

**High Risk Information:**

* Confidential [Company Name] information should only be stored within a shared folder on the [Company Name] network, within a user’s “My Documents” folder, or to a [Company Name] supplied encrypted laptop or memory stick. At no time should data be stored in any other location. Individual users’ “My Documents” folders are held in a secure location on the [Company Name] network.
* The use of personally identifiable data on portable devices, at home or from a remote location should be agreed as appropriate under the terms of the [Mobile Information Handling and Computing Policy]. This is to ensure that everyone is working in accordance with the [Company Name’s] data protection registration.
1. Access to read the document archives will only be granted to staff responsible for investigating system failure or system misuse, and then only to look at information as necessary to repair or protect the systems or to investigate use that may be in contravention of this AUP.

* Document files, web browsing logs, email or voicemail messages, however confidential or damaging, may have to be disclosed in court proceedings or during internal investigations if relevant to the issues being investigated.
* Access to a user's personal documents, either stored or held in an email mailbox, will only be granted to another user if a written request with appropriate reasons is received from the appropriate Director of [Company Name].
1. Infringement of copyright by copying or transmitting copyright material without permission of the copyright holder ("fair use" notwithstanding) is strictly forbidden. The [Company Name] name/logo may be used only for official [Company Name] documents and must be used in accordance with Corporate Identity guidelines.
2. The IT department schedules fileserver backups to enable recovery from any system failure.
* If staff do not have access to save their work to a [Company Name] fileserver, it is essential that they regularly copy any important work either to disk, a backup device, or another machine.
* Backup copies (including disks) must be stored in a secure area, e.g. fireproof safe.
* If access is given to an email account and it is not used for a [four-week] period, the account may be disabled. To re-enable the account, users must complete the appropriate documentation and forward it to the IT service desk; the request may be discussed prior to reactivating any access.
* Accounts not used for [3 months] (without prior warning) may be deleted under the assumption that the employee has left the organization.
* If users change job role, they should ensure computer access has been amended appropriate.
* If users change their job role, they should hand-over all relevant personal files and email messages to their line manager.
1. When informed by the HR department that a member of staff has ceased employment, the IT department will delete all personal information.

* Staff who cease employment with [Company Name], should take responsibility to hand over all appropriate personal computer files and email messages, either by forwarding them to a line manager, by copying them to a shared area, or by simply deleting them.
1. Remote control software is used by the IT department to connect and take control of a computer remotely. IT staff will not use this to connect to a computer without attempting to contact the user of the machine first. Access to this software is only permitted by IT staff or authorized System Managers.

* Remote access will not be given for other purposes, such as allowing managers to monitor their staff's work.
* Staff should not attempt to use any remote control software, nor allow external users or support staff to use it without the express permission of the IT department.
1. Access to the Internet is primarily provided for work-related purposes. Reasonable personal use is permitted provided this does not interfere with the performance of duties or adversely affect system performance. [Company Name] has the final decision on what constitutes excessive use. Staff may access some services (e.g. personal email or online banking) provided these are within the boundaries of incidental personal and acceptable use. [Company Name] cannot guarantee the privacy of staff accessing these facilities from work.

* Personal access to the Internet can be limited or denied by a manager. Staff must act in accordance with their manager’s local guidelines.
* The IT department has the right to withdraw internet access from any user and globally ban access to any site as appropriate, without warning.
* Unless specifically authorized, no member of staff may post messages under [Company Name’s] name to any newsgroup or chat room.
* Unless specifically authorized by the IT department, no member of staff may publish a website under the name of [Company Name] or featuring its logo.
* [Company Name] will not accept liability for personal legal (eg. libel) action resulting from staff misuse of the Internet.
* Access to file downloads will be restricted as necessary by IT to ensure system security.
* [Company Name] reserves the right, consistent with [local] law, to monitor all internet accesses, including but not limited to email and web access. No member of staff should consider information sent/received through the Internet as his/her private information.
* No member of staff may access, display, or download from internet sites that hold offensive material.
* Personal/employee identifiable data must not be published in any way on the Internet without the express consent of each and every individual concerned.
1. All software must be purchased, installed, and configured by the IT department; this includes all software packages, software upgrades, and add-ons, however minor. It also includes shareware, freeware, and any items downloaded from the Internet. Under no circumstances should any software be purchased or installed without the explicit agreement of the IT department.

* Do not violate the license agreement by making illegal copies of [Company Name] software. Anyone found doing so may be prosecuted under the [specific act applicable in your country] Act.
* Software not licensed to [Company Name] must not be loaded onto [Company Name] computers. Software licensing will be arranged and recorded by the IT department as part of the procurement and /or installation process.
* Users are not allowed to download software from the Internet or install from CD or disc without IT department authorization. Any unlicensed software found on a [Company Name] computer will be automatically deleted or disabled, and disciplinary action may be taken.
1. The use of any software package to access, modify, or analyze [Company Name’s] data for either work or personal purposes is forbidden without prior approval. The expectation by the [Information Governance committee] is that this use constitutes a short-term pilot.
* There should be no expectation that long-term use will be permitted or that [Company Name] will pay for personal software. Any information created or used must be stored appropriately based on the storage and retention rules that govern that information source.

**Low-Risk Information Specific Policy Statements**

1. [Company Name] allows and encourages the use social media to enhance both its personal visibility and image. Employees are expected to use these media types in a manner that is consistent with their employment contract.

**High-Risk Information Specific Policy Statements**

1. Under the Freedom of Information Act, the public has a general right to access all types of recorded information held by [Company Name]. Therefore, all staff have a duty to ensure that all records (manual and electronic, including emails) are recorded, preserved, and made available in accordance with the requirements of the Act.

*[This section is placed here for publically traded companies, non-governmental organizations and governmental departments. Most companies can delete this section.]*

# Non-Compliance

Clearly describe consequences (legal and/or disciplinary) for employee non-compliance with the policy. It may be pertinent to describe the escalation process for repeated non-compliance.

Violations of this policy will be treated like other allegations of wrongdoing at [Company Name]. Allegations of misconduct will be adjudicated according to established procedures. Sanctions for non-compliance may include, but are not limited to, one or more of the following:

1. Disciplinary action according to applicable [Company Name] policies;
2. Termination of employment; and/or
3. Legal action according to applicable laws and contractual agreements.

# Agreement

Include a section that confirms understanding and agreement to comply with the policy. Both signatures and dates are required. A sample statement is provided below.

I have read and understand the [name of policy]. I understand that if I violate the rules explained herein, I may face legal or disciplinary action according to applicable laws or company policy.

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Employee Name

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Employee Signature Date

# Revision History

|  |  |  |  |
| --- | --- | --- | --- |
| **Version ID** | **Date of Change** | **Author** | **Rationale** |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

For acceptable use of this template, refer to Info-Tech's [Terms of Use](http://www.infotech.com/terms). These documents are intended to supply general information only, not specific professional or personal advice, and are not intended to be used as a substitute for any kind of professional advice. Use this document either in whole or in part as a basis and guide for document creation. To customize this document with corporate marks and titles, simply replace the Info-Tech information in the Header and Footer fields of this document.