RANCHI UNIVERSITY, RANCHI

IT POLICY

Table of Content

ABBREVIATIONS

Abbreviations:

RU	Ranchi University
GoI	Government of India
IT	Information Technology
IA	Implementing Agency
LAN	Local Area Network
NAD	National Academic Depository
ABC	Academic Bank of Credits
ABA	Academic Bank Account

INTRODUCTION

Ranchi University, herein after Information Technology Policy will be IT Policy RU, will provide IT resources to support the educational, instructional, research, and administrative activities of the RU and to enhance the efficiency and productivity of the employees. These resources are meant as tools to access and process information related to their areas of work. These resources help them to remain well informed and carry out their functions in an efficient and effective manner.

This policy establishes specific requirements for the use of all IT resources at RU. This policy applies to all users of computing resources owned or managed by RU. Individuals covered by the policy include (but are not limited to) RU faculty and visiting faculty, staff, students, alumni, guests, external individuals, organizations, departments, offices, affiliated colleges and any other entity which fall under the management of RU accessing network services via RU's computing facilities.

For the purpose of this policy, the term ‘IT Resources’ includes all RU owned, licensed, or managed hardware and software, and use of the RU network via a physical or wireless connection, regardless of the ownership of the computer or device connected to the network.

Misuse of these resources will result in unwanted risk and liabilities for the RU. It is, therefore, expected that these resources are used primarily for RU related purposes and in a lawful and ethical way.

RU's Computing Facilities are related to symbolic computations, communications and network access, but not limited to, e-mail and Internet access. The Computer Centre undertakes security and monitoring measures to preserve the integrity and performance of its networking and computing resources.

RU is getting its Internet bandwidth from BSNL. Total bandwidth availability from BSNL source is 40 Mbps (leased line). RU has also got 1 Gbps connectivity under NKN Network of MHRD (NME-ICT) via BSNL. The whole campus is Wi-Fi enabled and Network facility is available for Teaching/Non-teaching Staff and all admitted Students of RU.

Online facilities available for all stakeholders via dynamic website and correspondence through official e-mail comes under vigilance and IT policy of the RU.

SCOPE

Scope

This policy governs the usage of IT Resources from an end user’s perspective. This policy is applicable to all individuals/ users/ entities, who use the IT Resources of RU.

This policy shall be applicable for the use of information, electronic devices, computing devices, and network resources of the RU. All faculty members, research scholars, students, employees, consultants, and other workers at RU are responsible for exercising rational judgment regarding appropriate and judicious use of ICT infrastructure in accordance with the following:

- The Information Technology Act, 2000 Government of India (GoI) including all subsequent Amendments.
- E-mail Policy of the GoI.
- Artificial Intelligence (AI) and Cyber Security policy of GoI will be adopted as amended time to time and will be applied.
- Any other policy or guidelines issued by the Government of India from time to time.

In addition to above, the RU can also devise guidelines for the expansion and use of ICT infrastructure. Such guidelines shall be open for amendments, as and when required. It may be noted that RU IT Policy applies to technology administered by the RU centrally or by the individual departments, to information services provided by the RU administration, or by the individual departments, or by individuals of the RU community, or by authorised resident or non-resident visitors on their own hardware connected to the RU network.

This IT policy also applies to the resources administered by the central administrative departments such as Library, Computer Centres, Laboratories, Offices of the RU recognised Associations/Unions, or hostels and guest houses, or residences wherever the network facility was provided by the RU.

Computers owned by the individuals, or those owned by research projects of the faculty, when connected to campus network are subjected to the Do’s and Don’ts detailed in the RU IT policy. Further, all the faculty, students, staff, departments, authorised visitors/visiting faculty and others who may be granted permission to use the RU’s information technology infrastructure, must comply with the Guidelines.

Violations of IT policy laid down by the RU by any RU member may even result in disciplinary action against the offender by the RU authorities. If the matter involves illegal action, law enforcement agencies may become involved.

Further, due to the dynamic nature of the Information Technology, Information Technology Tools, and Cyber Security in general, the latest updated rules/guidelines of GoI will be deciding.

OBJECTIVES & PRIVACY RIGHTS

Objective

The objective of this policy is to ensure security, prevent piracy, misuse of digital documents, and usages of information technology tools by the users of RU. Policy aims to protect the confidentiality, integrity, security, availability and performance of RU IT Resources.

Privacy Rights

An authorized user may use only the IT resources he/she has authorization.

1. No user should use another individual's account, or attempt to capture other users' passwords.
2. A user is individually responsible for appropriate use of all resources assigned to him/her, including the computer, the network address or port, software and hardware. Therefore, he/she is accountable to the RU for all use of such resources. As an authorized RU user, he/she should not engage in or enable unauthorized users to access the network by using IT resources of RU.
3. Users should make a reasonable effort to protect his/her passwords and to secure resources against unauthorized use or access. No user must attempt to access restricted portions of the network, an operating system, security software or other administrative applications without appropriate authorization by the system owner or administrator.
4. When an individual uses RU’s IT resources, and accepts any RU issued computing accounts, it means that the individual agrees to comply with this and all other computing related policies. It is the responsibility of the individual to keep oneself up-to-date on changes in the IT policy of RU and adapt to those changes as necessary from time to time.

ACCESS TO THE NETWORK

RU shall maintain two independent networks, i.e. Internet and Local Atea Network (LAN). Both the networks shall not have any physical connection/devices between them. End point compliance shall be implemented on both the networks to prevent unauthorized access to data.

1. Users shall not undertake any activity through any website or applications to bypass filtering of the network or perform any other unlawful acts which may harm the network's performance or security.
2. Computer Centre or any other Implementing Agency (IA) shall have the right to audit networks and systems at regular intervals, from the point of compliance to this policy.
3. IA/Nodal Agency, for security related reasons or for compliance with applicable laws, may access, review, copy or delete any kind of electronic communication or files stored on RU provided devices under intimation to the user. This includes items such as files, e-mails, posts on any electronic media, Internet history etc.
4. IA may monitor user's online activities on RU network, subject to such Standard Operating Procedures of GoI norms.
5. E-mail service authorized/notified by RU and implemented by the Computer Centre shall only be used for all official correspondence.
6. User shall comply with all the applicable provisions under the IT Act of GoI, while posting any information on social networking sites.
7. User shall adhere to the "Terms of Use" of the relevant social media platform/website, as well as copyright, privacy, defamation, contempt of court, discrimination, harassment and other applicable laws.
8. User shall report any suspicious incident as soon as possible to the competent authority.
9. User shall always use high security settings on social networking sites.
10. User shall not make any comment or post any material that might otherwise cause damage to RU's reputation.

SOFTWARE INSTALLATION AND LICENSING POLICY

Scope

Any computer purchases made by the individual departments/projects should make sure that such computer systems have all licensed software (operating system, antivirus software and necessary application software) installed.

Respecting the anti-piracy laws of the country, RU IT policy does not allow any pirated/unauthorized software installation on the RU owned computers and the computers connected to the RU campus network. In case of any such instances, RU will hold the department/individual personally responsible for any pirated software installed on the computers located in their department/individuals' rooms.

1. **Operating System and its Updating**
    1. Individual users should make sure that respective computer systems have their OS updated in respective of their service packs/patches, through Internet. This is particularly important for all MS Windows based computers (both PCs and Servers). Updating OS by the users helps their computers in fixing bugs and vulnerabilities in the OS that were periodically detected by the Microsoft for which it provides patches/service packs to fix them. Checking for updates and updating of the OS should be performed at least once in a week or so.
    2. RU as a policy encourages user community to go for open-source software such as Linux, Open office to be used on their systems wherever possible.
    3. Any MS Windows OS based computer that is connected to the network should access http://windowsupdate.microsoft.com web site for free updates. Such updating should be done at least once in a week. Even if the systems are configured for automatic updates, it is users' responsibility to make sure that the updates are being done properly.
2. **Antivirus Software and its updating**
    1. Computer systems used in the RU should have anti-virus software installed, and it should be active at all times. The primary user of a computer system is responsible for keeping the computer system compliant with this virus protection policy.
    2. Individual users should make sure that respective computer systems have current virus protection software installed and maintained.
    3. He/she should make sure that the software is running correctly. It may be noted that any antivirus software that is running on a computer, which is not updated or not renewed after its warranty period, is of practically no use. If these responsibilities appear beyond the end user's

technical skills, the end-user is responsible for seeking assistance from IT cell/IQAC RU or the service-providing agency.

3. Backups of Data

1. Individual users should perform regular backups of their vital data. Virus infections often destroy data on an individual's computer. Without proper backups, recovery of destroyed files may be impossible.
2. Preferably, at the time of OS installation itself, one can have the computer’s hard disk partitioned into two volumes typically C and D. OS and other software should be on C drive and user’s data files on the D drive. In case of any virus problem, generally only C volume gets corrupted. In such an event formatting only one volume, will protect the data loss. However, it is not a foolproof solution. Apart from this, users should keep their valuable data either in CD, External Hard-disc or other storage devices such as pen drives.

E-MAIL ACCOUNT USE POLICY

Email Account Use Policy

In an effort to increase the efficient distribution of critical information to all faculty, staff and students, and the RU's administrators, it is recommended to utilize the RU’s e-mail services, for formal RU communication and for academic & other official purposes.

E-mail for formal communications will facilitate the delivery of messages and documents to campus and extended communities or to distinct user groups and individuals. Formal RU communications are official notices from the RU to faculty, staff and students. These communications may include administrative content, such as human resources information, policy messages, general RU messages, official announcements, etc.

To receive these notices, it is essential that the e-mail address be kept active by using it regularly. Staff and faculty may use the email facility by logging on to https://www.ranchiuniversity.ac.in with their User ID and password. For obtaining the RU’s email account, user may contact IQAC RU for email account and default password by submitting an application in a prescribed proforma.

Terms of Services

Users may be aware that by using the email facility, the users are agreeing to abide by the following policies:

1. The facility should be used primarily for academic and official purposes and to a limited extent for personal purposes.
2. Using the facility for illegal/commercial purposes is a direct violation of the RU’s IT policy and may entail withdrawal of the facility. The illegal use includes, but is not limited to, the unlicensed and illegal copying or distribution of software, sending of unsolicited bulk e-mail messages. And generation of threatening, harassing, abusive, obscene or fraudulent messages/images.
3. While sending large attachments to others, user should make sure that the recipient has email facility that allows him to receive such large attachments.
4. User should keep the mail box used space within about 80% usage threshold, as ‘mail box full’ or ‘mailbox almost full’ situation will result in bouncing of the mails, especially when the incoming mail contains large attachments.
5. User should not open any mail or attachment that is from unknown and suspicious source. Even if it is from known source, and if it contains any attachment that is of suspicious nature or looks dubious, user should get confirmation from the sender about its authenticity before opening it. This is very much essential from the point of security of the user’s computer, as such messages may contain viruses that have potential to damage the valuable information on your computer.
6. Users should configure messaging software (Outlook Express/Netscape messaging client etc.,) on the computer that they use on permanent basis, so that periodically they can

download the mails in the mailbox on to their computer thereby releasing the disk space on the server. It is user's responsibility to keep a backup of the incoming and outgoing mails of their account.

7. User should not share his/her email account with others, as the individual account holder is personally held accountable, in case of any misuse of that email account.
8. User should refrain from intercepting, or trying to break into others email accounts, as it is infringing the privacy of other users.
9. While using the computers that are shared by other users as well, any email account that was accidentally left open by another user, should be promptly closed without peeping into its contents, by the user who has occupied that computer for its use.
10. Impersonating email account of others will be taken as a serious offence under the RU IT security policy.
11. It is ultimately each individual's responsibility to keep their e-mail account free from violations of RU's email usage policy.
12. All the mails detected as spam mails go into SPAM_MAIL folder of the respective users' mail accounts. Users are requested to open these folders periodically to check any important mail wrongly stamped as SPAM mail and went into this folder. It is recommended to empty this folder as frequently as possible.
13. The above laid down policies particularly 1 to 11 are broadly applicable even to the email services that are provided by other sources such as Hotmail.com, Yahoo.com etc., as long as they are being used from the RU's campus network, or by using the resources provided by the RU to the individual for official use even from outside.

WEB SITE HOSTING POLICY

1. Official Pages

Sections, departments and Teachers/Employees/Students may have pages on RU's official Web page. Official Web pages must conform to the IT Policy of the RU for Web site hosting.

As on date, the IT Cell/IQAC and Computer Centre at Central Library are responsible for maintaining the official web site of the RU viz., https://www.ranchiuniversity.ac.in only.

2. Affiliated Pages

Faculty/professional organizations may host Web pages for academic activities. Prior approval from the competent administrative authority via IQAC RU must be obtained for hosting such pages. Individual units reserve the right to discontinue the service and will provide reasonable advance notice to that affiliated organization.

3. Personal pages

The RU computer and network infrastructure is a limited resource owned by the RU. It is recognized that each individual faculty will have individual requirements for his/her pages. Hence, faculty may have their personal pages linked to official web site of the RU by sending a written request to INTERNET UNIT giving the details of the hyperlink of the URL that he/she wants to be added in the official web site of the RU. However, illegal or improper usage will result in termination of the hyperlink. The contents of personal pages must not violate any applicable export laws and regulations, must not constitute a copyright or trademark infringement, must not be used for commercial purposes, must not be used for political lobbying, and must not otherwise violate any local, state, or central government laws. Personal pages also will not include the hosting of pages for other individuals or groups.

Personal pages should explicitly mention that "Views expressed by him/her in their pages are exclusively their own and not that of the RU".

4. Web Pages for e-Learning

Though the RU does not have this facility as on this date, this Policy relates to future requirements for Web pages for e-Learning authored as a result of Teaching/Learning process. Faculty may have class materials (syllabi, course materials, resource materials, etc.) on the Web, linked through the appropriate department's pages.

Because majority of student pages will be published on the RU's Web for eLearning, it must reflect the academic mission, and be careful that the published material is not misrepresentative in any way by conflicting with official RU or other Web sites. If a student publishes a fictional Web site or a Web site modeled after an existing institution or corporation, the site must be clearly identified as a class project.

If Web pages developed for e-Learning become the part of the "official" RU page, they must be removed from the e-Learning departmental pages.

5. Policies for Maintaining Web Pages

1. Any information posted on official website must follow the IT policy of the RU. Web Pages must relate to the RU's mission.
2. Any page added/removed for any purpose/reason must immediately be brought into the notice of IQAC RU by sending the detail in hard copy as well as in soft copy wherever applicable.
3. Any non-functional/malfunctioning webpage(s) may be reported to the IQAC or Computer Centre of RU. The information will be forwarded to the Registrar RU by the IQAC or Computer Centre for remedial actions/decisions.

DATABASE USE POLICY

Database Policy

This Policy relates to the databases maintained by the RU administration under the RU’s e-Governance.

Its use must be protected even when the data may not be confidential. RU has its own policies regarding the creation of database and access to information and a more generic policy on data access. Combined, these policies outline the RU's approach to both the access and use of this RU resource.

A. Database Ownership: RU is the owner of all the RU's institutional data generated in the RU.

B. Custodians of Data: Individual Sections or departments generate portions of data that constitute RU’s database. They may have custodianship responsibilities for portions of that data.

Database Use Policy

Here are some general policy guidelines and parameters for Sections, departments and administrative unit data users:

a. The RU's data policies do not allow the distribution of data that is identifiable to a person outside the RU.

b. Data from the RU’s Database including data collected by departments or individual faculty and staff, is for internal RU purposes only.

c. One’s role and function define the data resources that will be needed to carry out one’s official responsibilities/rights. Through its data access policies, the RU makes information and data available based on those responsibilities/rights.

d. Data directly identifying a person and his/her personal information may not be distributed in any form to outside persons or agencies, including all government agencies and surveys and other requests for data. All such requests are to be forwarded to the Office of the RU Registrar.

e. Requests for information from any courts, attorneys, etc. are handled by the Registrar Office of the RU and departments should never respond to requests. All requests from law enforcement agencies are to be forwarded to the Office of the RU Registrar for response.

f. At no time may information, including that identified as ‘Directory Information’, be released to any outside entity for commercial, marketing, solicitation or other purposes.

g. This includes organizations and companies which may be acting as agents for the RU or its departments.

h. All reports for UGC, MHRD and other government agencies will be prepared/compiled and submitted by the Registrar, CCDC, Controller of Examinations, DSW, AISHE Coordinator, Nodal

Officer RUSA, and Finance officer of the RU. IQAC RU will use these data for storage and retrieval uses and for submitting the Annual Quality Assurance Report (AQAR) each year for NAAC assessment and for the preparation of Self Study Report (SSR).

i. Database users who repackage data for others in their unit must inform the recipients of the above data access issues.

j. Tampering of the database by the department or individual user comes under violation of IT policy. Tampering includes, but not limited to:

    a) Modifying/deleting the data items or software components by using illegal access methods.

    b) Modifying/deleting the data items or software components deliberately with ulterior motives even by authorized individuals/ departments.

    c) Causing database or hardware or system software crash thereby destroying the whole of or part of database deliberately with ulterior motives by any individual.

    d) Trying to break security of the Database servers.

Such data tampering actions by RU member or outside members will result in disciplinary action against the offender by the RU authorities. If the matter involves illegal action, law enforcement agencies may become involved.

RESPONSIBILITIES OF RU COMPUTER CENTER

Responsibilities of RU Computer Center

In addition to the responsibilities already assigned with, the Computer Centre will work in association with IQAC RU regarding formatting/ storage/ hoisting data at website and other website related activities. The Computer Center situated at the Central Library may coordinate with service engineer to resolve the problem with joint effort without failing to inform CCDC RU. This task should not be left to the individual user.

A. Maintenance of Computer Hardware & Peripherals

Computer Center is responsible for maintenance of the RU owned computer systems and peripherals that are either under warranty or annual maintenance contract, and whose responsibility has officially been entrusted to this Cell.

B. Receiving Complaints

Computer Center may receive complaints from the users if any of the computer systems or peripherals that are under maintenance through them are having any problems.

The designated person in Computer Center receives complaints from the users of these computer systems and coordinates with the service engineers of the respective brands of the computer systems to resolve the problem within a reasonable time limit.

C. Scope of Service

Computer Center will be responsible only for solving the hardware related problems or OS or any other application software that were legally purchased by the RU and was loaded by the company. All cases must be reported to the CCDC RU for assistance.

D. Installation of Un-authorized Software

Computer Center or its service engineers should not encourage installing any unauthorized software on the computer systems of the users. They should strictly refrain from obliging such requests.

E. Reporting IT Policy Violation Incidents

If Computer Center or its service engineers come across any applications that are interfering with the network operations or with the IT policies of the RU, such incidents should be brought to the notice of the RU authorities.

F. Reporting incidents related to Network Operations

When the network port of any particular computer system is turned off due to virus or related activity that is affecting the network performance, the same will be informed to the Computer Center. After taking necessary corrective action Computer Center or service engineers should inform CCDC RU about the same.

G. Rebuilding the Computer System

When the service engineers reformat the computer systems and re-install OS and other application software, care should be taken to give the same hostname, IP address, network Mask, gateway as it was having earlier. Further, after installing the OS all the patches/latest service pack should also be properly installed. In case of anti-virus software, service engineers should make sure that its latest engine and pattern files are also downloaded from the net.

Further, before reformatting the hard disk, dump of only the data files should be taken for restoring it back after proper re-installation. Under no circumstances, software files from the infected hard disk dump should be used to write it back on the formatted hard disk.

H. Data Backup, Security, and Disclaimer

Computer Center will not be liable for the loss or corruption of data on the individual user’s computer as a result of the use and/or misuse of his/her computing resources (hardware or software) by the user or from any damage that may result from the advice or actions of a Computer Center staff member in the process of helping the user in resolving their network/computer related problems.

Although Computer Center make a reasonable attempt to provide data integrity, security, and privacy, the User accepts full responsibility for backing up files in the assigned Net Access ID, storage space or email Account. In addition, Computer Center makes no guarantee concerning the security or privacy of a User's electronic messages.

VIDEO SURVEILLANCE POLICY

The system

a. The system comprises: Fixed position cameras; Pan Tilt and Zoom cameras; Monitors: Multiplexers; digital recorders; SAN/NAS Storage; Public information signs.

b. Cameras will be located at strategic points on the campus, principally at the entrance and exit point of sites and buildings. No camera will be hidden from view and all will be prevented from focusing on the frontages or rear areas of private accommodation.

c. Signs will be prominently placed at strategic points and at entrance and exit points of the campus to inform staff, students, visitors and members of the public that a CCTV/IP Camera installation is in use.

d. Although every effort has been made to ensure maximum effectiveness of the system it is not possible to guarantee that the system will detect every incident taking place within the area of coverage.

Purpose of the system

a. The system has been installed by RU with the primary purpose of reducing the threat of crime generally, protecting universities premises and helping to ensure the safety of all staff, students and visitors consistent with respect for the individuals' privacy. These purposes will be achieved by monitoring the system to:

   - Deter those having criminal intent
   - Assist in the prevention and detection of crime
   - Facilitate the identification, apprehension and prosecution of offenders in relation to crime and public order
   - Facilitate the identification of any activities/event which might warrant disciplinary proceedings being taken against staff or students and assist in providing evidence to managers and/or to a member of staff or student against whom disciplinary or other action is, or is threatened to be taken.
   - In the case of security staff to provide management information relating to employee compliance with contracts of employment

b. The system will not be used:

   - To provide recorded images for the world-wide-web.
   - To record sound other than in accordance with the policy on covert recording.
   - For any automated decision taking

Covert recording

a. Covert cameras may be used under the following circumstances on the written authorization or request of the Senior officer, Registrar and where it has been assessed by the Head of Security and Facilities Services and the Data Protection Officer

- That informing the individual(s) concerned that recording was taking place would
- seriously prejudice the objective of making the recording; and
- That there is reasonable cause to suspect that unauthorized or illegal activity is taking
- place or is about to take place.

a. Any such covert processing will only be carried out for a limited and reasonable period of time consistent with the objectives of making the recording and will only relate to the specific suspected unauthorized activity.

b. The decision to adopt covert recording will be fully documented and will set out how the decision to use covert recording was reached and by whom.

The Security Control Room

a. Images captured by the system will be monitored and recorded in the Security Control Room, "the control room", twenty-four hours a day throughout the whole year. Monitors are not visible from outside the control room.

b. No unauthorized access to the Control Room will be permitted at any time. Access will be strictly limited to the duty controllers, authorized members of senior management, police officers and any other person with statutory powers of entry.

c. Staff, students and visitors may be granted access to the Control Room on a case-by-case basis and only then on written authorization from the Registrar. In an emergency and where it is not reasonably practicable to secure prior authorization, access may be granted to persons with a legitimate reason to enter the Control Room.

d. Before allowing access to the Control Room, staff will satisfy themselves of the identity of any visitor and that the visitor has appropriate authorization. All visitors will be required to complete and sign the visitors' log, which shall include details of their name, their department or organization they represent, the person who granted authorization and the times of entry to and exit from the centre. A similar log will be kept of the staff on duty in the Security Control Room and any visitors granted emergency access.

Security Control Room Administration and Procedures

a. Details of the administrative procedures which apply to the Control Room will be set out in a Procedures Manual, a copy of which is available for inspection by prior arrangement, stating the reasons for the request.

b. Images of identifiable living individuals are subject to the provisions of the Prevailing Data Protection Act; the Control Room Supervisor is responsible for ensuring day to day compliance with the Act. All recordings will be handled in strict accordance with this policy and the procedures set out in the Procedures Manual.

Staff

a. All staff working in the Security Control Room will be made aware of the sensitivity of handling CCTV/IP Camera images and recordings.

b. The Control Room Supervisor will ensure that all staff are fully briefed and trained in respect of the functions, operational and administrative, arising from the use of CCTV/IP Camera.

Recording

a. Digital recordings are made using digital video recorders operating in time lapse mode. Incidents may be recorded in real time.

b. Images will normally be retained for fifteen days from the date of recording, and then automatically over written and the Log updated accordingly. Once a hard drive has reached the end of its use it will be erased prior to disposal and the Log will be updated accordingly.

c. All hard drives and recorders shall remain the property of RU until disposal and destruction.

Access to images

a. All access to images will be recorded in the Access Log as specified in the Procedures Manual

b. Access to images will be restricted to those staff need to have access in accordance with the purposes of the system.

Access to images by third parties

a. Disclosure of recorded material will only be made to third parties in strict accordance with the purposes of the system and is limited to the following authorities:

   - Law enforcement agencies where images recorded would assist in a criminal enquiry and/or the prevention of terrorism and disorder
   - Prosecution agencies
   - Relevant legal representatives
   - The media where the assistance of the general public is required in the identification of a victim of crime or the identification of a perpetrator of a crime
   - People whose images have been recorded and retained unless disclosure to the individual would prejudice criminal enquiries or criminal proceedings.
   - Emergency services in connection with the investigation of an accident.

b. CCTV/IP Camera digital images, if they show a recognizable person, are personal data and are covered by the Data Protection Act. Anyone who believes that they have been filmed by C.C.T.V. /IP Camera is entitled to ask for a copy of the data, subject to exemptions contained in the Act. They do not have the right of instant access.

c. A person whose image has been recorded and retained and who wishes access to the data must apply in writing to the Data Protection Officer. Subject Access Request Forms are obtainable from the Security Office, between the hours of 1020 and 1400 and 1430 to 1800 Monday to Saturday, except when RU is officially closed or from the Data Protection Officer, the Records Office during the same hours.

d. The Data Protection Officer will then arrange for a copy of the data to be made and given to the applicant. The applicant must not ask another member of staff to show them the data, or ask anyone else for a copy of the data. All communications must go through the RU Data Protection Officer. A response will be provided promptly and in any event within forty days of receiving the required fee and information.

e. The Data Protection Act gives the Data Protection Officer the right to refuse a request for a copy of the data particularly where such access could prejudice the prevention or detection of crime or the apprehension or prosecution of offenders.

f. All such requests will be referred to the Security Control room Supervisor or by the Data Protection Officer.

g. If it is decided that a data subject access request is to be refused, the reasons will be fully documented and the data subject informed in writing, stating the reasons.

Request to prevent processing

a. An individual has the right to request a prevention of processing where this is likely to cause substantial and unwarranted damage or distress to that or another individual.

b. All such requests should be addressed in the first instance to the Security Control Room Supervisor or the Data Protection Officer, who will provide a written response within 21 days of receiving the request setting out their decision on the request. A copy of the request and response will be retained.

Complaints

a. It is recognized that members of RU and others may have concerns or complaints about the operation of the system. Any complaint should be addressed in the first instant to the Security Control Room supervisor. If having exhausted the steps set out, the complaint remains unresolved; the complainant may invoke Universities Centralized Complaints Procedure by obtaining and completing a RU Complaints Form and a copy of the procedure.

b. Complaints forms may be obtained from the Security Office, and the Registrar's Office.

a. Concerns or enquiries relating to the provisions of the prevailing Data Protection Act may be addressed to the Data Protection Officer.

b. These rights do not alter the existing rights of members of RU or others under any relevant grievance or disciplinary procedures.

Compliance monitoring

a. The contact point for members of RU or members of the public wishing to enquire about the system will be the Security Office which will be available during the hours of 1020 and 1400 and 1430 to 1800 Monday to Saturday (except second and fourth Saturday) except when RU is officially closed.

b. Upon request enquirers will be provided with:

- A summary of this statement of policy
- An access request form if required or requested
- A subject access request form if required or requested
- A copy of the RU central complaints procedures

All documented procedures will be kept under review and a report periodically made to the Estates Management Committee. The effectiveness of the system in meeting its purposes will be kept under review and reports submitted as required to the Estates Management Committee.