
Imperial College

Code of Practice 3: Inspection of Electronic Communications and Data

Doc. Ref. : Code of Practice 3: Inspection of Electronic Communications and Data
Version : 4.1
Status : Approved
Date : 28/03/2022
Approved by : The Information Governance Steering Group
Review by : 31 March 2024

1. SCOPE

- 1.1 The purpose of this Code of Practice is to prescribe the circumstances under which the College may monitor or intercept electronic communications. It applies to staff, students and external third parties that have access to or permission to use the College's electronic communications facilities.

2. MONITORING ELECTRONIC COMMUNICATIONS

- 2.1 Electronic communications are broadly telephone calls, fax messages, all types of electronic messages including e-mails, instant messages, SMS or other short messages, tweets, published web contents including wikis, blogs, posts on messaging platforms, etc. The College does not, as a matter of course, undertake general monitoring of the contents of staff or student electronic communications. Moreover, the College does not routinely undertake random sampling or general scanning of electronic communications through human intervention. However automated computerised scanning of email traffic is performed for the purpose of intercepting unsolicited bulk email (commonly referred to as "spam") and potentially damaging message content (computer viruses, attempts at financial fraud etc.)
- 2.2 Paragraph 6 in the College's Information Security Policy explains that in accordance with [the "Telecommunications \(Lawful Business Practice\) \(Interception of Communications\) Regulations 2000"](#), made under [the "Regulation of Investigatory Powers Act 2000"](#) (RIPA) 2000, the College will exercise its right to intercept and monitor electronic communications received by and sent from the College for the purposes permitted under those Regulations.
- 2.3 If an organisation intercepts a communication on its system without legal authority, the sender or the recipient of the communication will be able to obtain an injunction or, if they can show that they suffered a loss as a result of the interception, sue for damages. RIPA also establishes the circumstances in which it is lawful to intercept communications. It authorises interception in cases where the interceptor has reasonable grounds to believe that both the sender and intended recipient have consented. It also provides for the Secretary of State to make "Lawful Business Practice" Regulations setting out the circumstances in which organisations can lawfully intercept communications without consent.
- 2.4 Of relevance to Imperial College is [the "Telecommunications \(Lawful Business Practice\) \(Interception of Communications\) Regulations 2000"](#). This allows organisations to intercept, without consent, for purposes such as recording evidence of transactions, ensuring regulatory compliance, detecting crime or unauthorised use and ensuring the effective operation of their telecommunications systems. Organisations will not need to gain consent before intercepting for these purposes although they must have informed the users of the systems that interceptions may take place.
- 2.5 The purposes for which organisations will be able to intercept without consent under the Regulations are listed below. Depending on circumstances Imperial College may make use of some or all of these purposes:
 - 2.5.1 Establishing the existence of facts relevant to the organisation, for example keeping records of transactions and other

- communications in cases where it is necessary or desirable to know the specific facts of the communication.
- 2.5.2 Ascertaining compliance with regulatory or self regulatory practices or procedures relevant to the organisation, for example monitoring as a means to check that the organisation is complying with regulatory or self regulatory rules or guidelines.
 - 2.5.3 Ascertaining or demonstrating standards which are or ought to be achieved by persons using the system, for example monitoring for purposes of quality control or staff training.
 - 2.5.4 Preventing or detecting crime for example, monitoring or recording to detect fraud, computer misuse or other illegal activities.
 - 2.5.5 Investigating or detecting the unauthorised use of the systems, for example monitoring to ensure that employees do not breach College rules e.g. as listed in Section 11: "Conditions of Use of IT Resources (Acceptable Use Policy)" in [Information Security Policy](#).
 - 2.5.6 Ensuring the effective operation of the system, for example monitoring for and deleting viruses, checking for and stopping other threats to the system e.g. hacking or denial of service attacks, monitoring automated processes such as net flow logs, e-mails logs, caching activity and load distribution.
 - 2.5.7 Determining whether or not the communications are relevant to the organisation, for example checking email accounts to access communication in staff absence.
 - 2.5.8 In the case of communications to a confidential anonymous counselling or support help line, for example monitoring calls to confidential, welfare help lines in order to protect or support help line staff.
- 2.6 The College intends to make interceptions for the purposes authorised under the Regulations, and has made reasonable efforts to inform members of College, who may use its system, that communications may be intercepted.
- 2.7 Users of College communications should be aware that ICT System and Network Administrators, from time to time, monitor transmissions or observe transactional information to ensure proper functioning of College IT services. On these and other occasions such personnel might, inadvertently, become aware of the contents of electronic communications. Except as provided elsewhere in this Code of Practice or by law, personnel are not permitted to intentionally examine the contents of transactional information or disclose or otherwise use what they have seen, heard, or read. If, however, violations of College policy or law are discovered they must be reported to College authorities.
- 2.8 The contents of electronic communications and transactional records may be inspected to redirect or dispose of otherwise undeliverable electronic communications, e.g. that are addressed to Postmaster or Webmaster. Such unavoidable inspection of electronic communications is limited to the minimal level of examination required to route the otherwise undeliverable electronic communication to its intended recipients. Re-routed electronic communications must be accompanied by notification to the recipient that the electronic communication has been inspected for such purposes.

3. INSPECTION OF ELECTRONIC DATA

- 3.1 It may be necessary, from time to time, for the College to investigate the data on networked or stand-alone College owned storage, including but not limited to individuals' College emails, documents and files in local, home or group drives, account information, and logs, e.g. access logs to College systems or premises. Furthermore, by connecting a privately owned device to the College network, the user consents to allow the College to inspect it in accordance with section 6 "Monitoring Electronic Communications" of College's Information Security Policy. Any such inspection actions taken and any subsequent disclosures shall be in full compliance with the law, particularly the UK General Data Protection Regulation (GDPR), the Data Protection Act 2018 and applicable College policies.
- 3.2 Under normal circumstances, the user's consent will be sought by the College prior to any inspection being carried out on data held by or related to individuals, e.g. College email accounts, home or local drives, access logs, etc. However, in the following circumstances inspection will be carried out even though the user has not given consent:
- 3.2.1 when there is a legal requirement to do so;
 - 3.2.2 when there are reasons to believe that violations of law or of College policies may have taken place, e.g. where there is reliable evidence as distinguished from rumour or gossip;
 - 3.2.3 when there are compelling/emergency circumstances, for example when failure to act might result in significant bodily harm, significant property loss or damage, loss of significant evidence of one or more violations of law or of College policies, or significant liability to the College or to members of the College community;
 - 3.2.4 when failure to act could seriously hamper the ability of the College to function administratively or to meet its teaching/research and related obligations.
- 3.3 If inspection of data held by or related to individuals is required for business reasons while the account holder is away from the College, the consent of the account holder must first be sought. If the account holder cannot be contacted, the Head of Department and the Data Protection Office must jointly authorise the inspection in writing. Both a record of the measures taken to obtain consent, and the basis for allowing the inspection must be recorded.
- 3.4 In instances where data held by or related to individuals are to be lawfully inspected due to circumstances listed in section 3.1 without the user's consent, the following shall apply:
- 3.4.1 **Emergency Circumstances:** The minimal perusal of contents and the minimal action necessary to resolve the emergency may be taken immediately without authorisation, but appropriate authorisation must then be sought without delay and recorded as per paragraph 3.2.4;
 - 3.4.2 **All other circumstances:** Inspection must be subject to the prior joint authorisation, in writing, by the Head of Department and the College Secretary.
 - 3.4.3 **Encrypted Information.** When a system is found to contain encrypted information, a relevant decryption key must be provided upon request.
 - 3.4.4 **Data created by or related to staff/students no longer employed by or studying at the College left on College systems is the property**

Commented [RS1]: Im guessing this should be 3.2 instead

of the College. It is not necessary to seek the permission of the former member of staff/student before such information can be inspected. Authorisation to view information must be sought jointly from the Head of Department and the Data Protection Office as per section 3.2.

- 3.5 Once authorisation has been granted, any information found on a system shall be treated in the following manner:
- 3.5.1 College/Work related material shall be dealt with in line with normal working practices and retained or deleted as necessary.
 - 3.5.2 Material that appears to be of a personal nature will only be inspected if there is a legitimate business reason for doing so.
 - 3.5.3 Members of College are responsible for removing any personal information from their electronic documents and emails before their departure.
- 3.6 Privacy. Any inspection, authorized under this CoP, shall be conducted with due regard to the right to privacy. Material that appears to be private shall be subject to the minimal inspection required to conclude the search. Any confidential information encountered which is not related to the purpose for which the search was undertaken shall not be disclosed to any party, and shall remain confidential. However, if material is accidentally discovered in the course of an inspection which is either illegal or contravenes College policies, the matter will be referred to the College Secretary, who may authorise further investigation.

Commented [RS2]: As above, im guessing this should be 3.2)

Version History

Version/Status	Release Date	Comments
1.0/Approved	May 2012	Approved
1.1/Revised – In Review	May 2016	Fully revised version following findings report by Information Governance Audit in 2015. Reviewed by John Neilson, College Secretary and Mike Russell, CIO
1.2/In Review	July 2016	Reviewed by IGSG
2.0/Approved	November 2016	Approved by the Provost Board
2.1/In Review	November 2017	Reviewed by Okan Kibaroglu and Tim Rodgers
3.0/Approved	May 2018	Published
3.1/In Review	March 2019	Reviewed by ICT Governance and Security
4.0/Approved	January 2021	Published linked to InfoSec Policy v6.0.
4.1/In review	March 2022	3.1 updated legislation name 3.3 remove College Secretary and reference D 3.4 remove College Secretary and reference D 3.4.4 remove College Secretary and reference