Projectcode	-
Version	Final
Date	Version 28 January 2019
Author	HR
Owner	-
Comissioned by	Erasmus MC's Executive Board

Erasmus MC Code of Conduct for the use of Internet and ICT Facilities

Introduction

Many Erasmus MC Employees use the Internet and ICT Facilities. Due care should be exercised when using these facilities. Using the Internet and ICT Facilities, including email and Mobile Devices, has many advantages but also entails some risks. That is why we have drawn up this Code of Conduct with rules and regulations for the use of the Internet and ICT Facilities. In drawing up this Code of Conduct we tried to find a good balance between monitoring responsible use of the computer facilities and the protection of Employees' privacy. Violation of this Code of Conduct may lead to a breach of duty in accordance with clause 11.1 of the Collective Labour Agreement.

We also had to consider the fact that third parties work for Erasmus MC and use its Internet and ICT Facilities. The Code of Conduct will also be declared applicable to these third parties in the contract entered into with them.

Generally speaking, if the use of the Internet and ICT Facilities or the monitoring thereof involves the processing of Personal Data, any processing should comply with the requirements of the General Data Protection Regulation ("GDPR"). In any event, the processing will be recorded in Erasmus MC's Record of Processing Activities. If it is subsequently established that such processing involves privacy risks, a privacy impact assessment in accordance with the GDPR may have to be carried out.

Erasmus MC will not make improper use of the options to audit Employees' use of the Internet and ICT Facilities.

Objectives

The purpose of this Code of Conduct is to set and disclose rules and regulations for the use of the Internet and ICT Facilities, including the mutual rights and obligations of the employer and the Employee. Additionally, we aim to restrict the following risks and prevent:

- An overload and abuse of the Internet and ICT Facilities.
- Incidents or damage due to the use of the Internet and ICT Facilities.
- Impermissible disclosure to third parties of Confidential Information about patients, Employees, students or, in general, Erasmus MC.

Definition of terms

Employee:	a natural person employed by Erasmus MC or who is otherwise appointed as working under the responsibility of Erasmus MC.
Personal Data:	any information about an identified or an identifiable person, "the data subject". Identifiable means a natural person who may be identified, directly or indirectly, by reference to an identifier such as a name, an identification number, location data, an online identifier or to a combination of one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

Automated Information Systems:	data-processing systems that collect, process, edit, store, transfer and provide information used in Erasmus MC's business processes where use is made of the Internet and ICT Facilities.
Confidential Information:	Confidential Information which an Employee knows or should understand may not be disclosed to others without authorisation. This includes Personal Data as defined in the GDPR including data relating to patients, Employees, research and competitively sensitive information.
Operators:	employees of the I&T division of the service company entrusted with supervising and managing the operation of Erasmus MC's Internet and ICT Facilities. This includes among other things, the ICT service desk staff, management of the work stations, servers, network, making back-ups etc.
CERT:	Computer Emergency Response Team.
Internet and ICT Facilities:	all ICT devices that are used to execute Erasmus MC's business processes, including: devices and Mobile Devices owned by or on loan from Erasmus MC, software, networks, devices and Mobile Devices owned by the Employee but used for work purposes.
Mobile Devices:	laptop, tablet, smartphone, digital data carriers and any other handsets with internet and ICT facilities.
Spam:	unwanted messages spread via email and Social Media.
Social Media:	online platforms on which users, with minimal or no influence from professional editors, create content. Examples of these platforms are weblogs, video sites and photo sites, microblogs and social network sites. The best known sites are You Tube, Pinterest, Twitter and Facebook.

1. Scope

This Code of Conduct applies to the Employee who, using the Internet and ICT Facilities, gains access to the Automated Information Systems provided by or on behalf of Erasmus MC.

The Code of Conduct also applies if it has been declared applicable in a contract with a third party and this third party gains access, by using the Internet and ICT Facilities, to the Automated Information Systems provided by or on behalf of Erasmus MC. In that case the word 'Employee' in this Code of Conduct should be read as 'third party'.

2. General use

2.1 The Internet and ICT Facilities which have been provided to the Employee are intended to be used for work purposes. Private use is only permitted if this does not negatively affect his daily work or damage Erasmus MC's Internet and ICT Facilities or the performance thereof.

2.2. Using or exploiting Erasmus MC's Internet and ICT Facilities for commercial purposes other than those arising from performing tasks and duties related to the job is not permitted.

2.3 It is not permissible to produce, access, store, spread or disclose information which is contrary to the law or good morals (e.g. pornographic material), information that affects the good name of Erasmus MC or discriminating, incendiary, offensive or threatening information, using Erasmus MC's Internet and ICT Facilities, unless this is necessary from the point of view of medical treatment and/or scientific research.

2.4 Unauthorised copying or disclosure to third parties of software, hardware, data files or documentation provided by Erasmus MC is not permitted.

2.5 The Employee will not engage in or try to engage in activities that undermine the continuity or the security of Erasmus MC's Internet and ICT Facilities.

2.6 In the Employee's absence he will make sure that his computer/Mobile Devices are completely shut down or protected with a screensaver and a password in accordance with Erasmus MC's 'clear desk' and 'clear screen' policy. Both policies can be found on the Intranet.

2.7 When digital data carriers (such as USB-sticks) are used, the storage of Confidential Information on these carriers must be encrypted. The Employee can find instructions for this on Erasmus MC Service Portal.

2.8 When printing Confidential Information the Employee must ensure that this information does not reach others.

3. Access to the Internet and ICT Facilities

3.1 Access to Erasmus MC's Internet and ICT Facilities will be provided on the basis of a username (micro section number) and a personal password or other similar means of identification and authentication (such as smart cards and tokens). These are personal and non-transferable.

3.2 The Employee ensures that:

- the password is not disclosed to others;
- the personal means of identification and authentication are not used by others;
- if he discovers that the combination of his username and password or other means of identification and authentication has been misused, he will immediately inform the ICT service desk of this and change his password.

3.3 The Employee will, at regular intervals, be requested (via the system) to change his password.

3.4 The password linked to department accounts or accounts shared by multiple people, will be shared with the people who need to have access to these accounts. Article 3.2 applies accordingly to third parties who do not need to have access to this shared account. The person responsible for the shared account will arrange and stop access to it, including password changes if the group of people who have access changes. This person notifies users with whom they may share the

password and, if applicable, will make agreements with the users of the shared account to ensure the protection of Personal Data.

4. Rules and conditions for the use of email and internet

4.1 The use of the email address provided to an Employee in a personal capacity, is strictly private. Non-personal email addresses may be shared by several Employees but one Employee is always appointed as the contact person for this email address. Article 3.2 applies accordingly.

4.2 The Employee is not permitted to:

a) Use an email address which is not linked to him unless the Employee has been authorised by the rightful user of this email address through his email account.
b) Send Spam using Erasmus MC's Internet and ICT Facilities.
c) Bully, offend, stalk, threaten, malign or otherwise damage another person using Erasmus MC's Internet and ICT Facilities.
d) Deliberately read, copy, change, forward or destroy email messages intended for other Employees without permission. If an Employee receives an email message which was not intended for him he forwards this message to the person it was intended for and/or informs the sender of this and deletes the email from his mailbox.
e) Send information which is contrary to the law or good morals (e.g. pornographic material), information that affects the good name of Erasmus MC and/or discriminating, incendiary, offensive or threatening information, unless this is necessary from the point of view of medical treatment and/or scientific research.
f) Send unencrypted Personal Data, including data relating to patients and Employees', to an email address outside Erasmus MC or to an Erasmus MC email address whose receiver is not authorised to obtain this information. And in general, provide unencrypted Confidential Information without a legitimate purpose and/or a legal ground, via the internet and/or distribute this unencrypted information via public networks.
g) Send Employees or groups of Employees electronic chain letters or virus warning messages.
h) Copy and/or download through Erasmus MC's facilities copyright-protected material, including software, texts, footage or music or provide material belonging to Erasmus MC or third parties without the permission of the entitled party.

4.3 When downloading material, the Employee must do everything in his power to prevent the downloading of, for example, viruses and not endanger the availability of the Internet and ICT Facilities for others.

4.4 Sending Confidential Information using the internal network (to and from an Erasmus MC email address (@erasmusmc.nl)) if both the sender and the receiver are entitled to this information, is permitted.

4.5 Confidential Information available on the Erasmus MC intranet may not be copied or distributed in any way by an Employee.

5. The use of Social Media

5.1 Social Media users should take account of Erasmus MC's good reputation and that of the people involved with it. Employee's private opinions may easily be mistaken

for official Erasmus MC viewpoints, and it is up to the Employee to prevent this from happening. Article 2.1 applies in full to the use of Social Media.

5.2 Sharing knowledge and information is permitted, provided that it does not concern Confidential Information or Personal Data for which no permission to share has been given, and provided that it does not harm Erasmus MC or others involved with it.

5.3 The Employee is personally responsible for the content he posts on Social Media.

5.4 Be aware that published texts and remarks remain open to the public for an indefinite period of time, even after the message has been deleted.

5.5 Employees are not permitted to share photos, film recordings and sound recordings from Erasmus MC-related events on Social Media, unless they have been given explicit permission to do so by the persons involved and Erasmus MC's Communication Department.

5.6 Employees are to abide by the prevailing standards of decency. If those standards of decency are breached (for example: by bullying, hurting, stalking, threatening, maligning or otherwise damaging another person) Erasmus MC will be entitled to take appropriate measures.

6. The use of Mobile Devices provided

6.1 The Employee may be provided with Mobile Devices for work purposes. The Employee must then sign a loan agreement.

6.2 In the event of theft or loss of the Mobile Devices, the Employee should immediately notify the ICT Service desk of this and report it to the police. If a data leak occurs it must be reported in accordance with the applicable procedure within Erasmus MC (see Intranet).

6.3 The Employee who wants to use his Mobile Device to access his calendar and email or who wants to access the intranet via a non-Erasmus MC network, can only do so by installing and using a board-approved application(s), (app(s)), on his Mobile Device. This/These app(s) is/are designed to keep Confidential Information within Erasmus MC's secure environment. The installation of this/these app(s) must be approved by a manager.

6.4 The Employee may not store Confidential Information on (the hard drive) of his Mobile Device unless this information is encrypted. Instructions on how to encrypt documents can be found on Erasmus MC's Service Portal.

7. The use of Mobile Devices owned by an Employee

7.1 The Employee may use his personal Mobile Devices for work purposes. The Employee remains responsible for his own devices and must ensure that they have the necessary security, such as an access code and encryption. Erasmus MC does not offer support for maintenance and management except for the application(s) required and provided by Erasmus MC.

7.2 The Employee who wants to use his personal Mobile Device to access his calendar and email or who wants to access the intranet via a non-Erasmus MC network, can only do so by installing and using a board-approved application(s), (app(s)), on his Mobile Device. This/These app(s) is/are designed to keep Confidential Information within Erasmus MC's secure environment. The installation of this/these app(s) must be approved by a manager.

7.3 In the event of theft or loss of the personal Mobile Device equipped with the required application(s), the Employee should immediately notify the ICT Service desk of this so it can remotely remove Erasmus MC application(s) and information. If a data leak is suspected it must be reported in accordance with the applicable procedure within Erasmus MC (see Intranet).

7.4 The Employee may not store Confidential Information, with the exception of the application(s) referred to in article 7.2, on (the hard drive) of his personal Mobile Device unless this information is encrypted. Instructions on how to encrypt documents can be found on Erasmus MC's Service Portal.

8. Non-personal monitoring of email and internet

8.1 A non-personal and automated monitoring of the use of email and internet (including private email messages sent through Erasmus MC network) will take place as part of the system and network security in order to prevent and detect violations of the Code of Conduct as drawn up in these regulations. This monitoring is mainly automated and takes place 24 hours per day.

8.2 The automated and non-personal monitoring comprises:

a. scanning for dangerous file formats and virus signatures;
b. scanning for the automatic forwarding of emails to non-Erasmus MC email addresses;
c. scanning for software downloads;
d. analysing the traffic data of email and internet use in the interests of cost control and capacity management;
e. retrospective content scanning of email messages and internet traffic for racist and sexually charged content or unauthorised disclosure of Confidential Information.

8.3 The content scanning referred to in paragraph 2e focusses on keywords and graphic files with certain characteristics. Internet traffic can also be checked on the basis of the names of visited sites.

8.5 Logging takes place within the context of system administration and network management. This enables us to record which data has been processed, collected, examined, changed or deleted in an IT-system. Log files aim to enhance the integrity and the security of data. They can also provide valuable information on, for example, peak load or existing software bugs. This information will be stored for a maximum period of six months.[1]

9. Personal monitoring

9.1 If the non-personal monitoring gives reason to believe or results in concrete facts or circumstances that an Employee is not complying with the Code of Conduct and/or

[1] There is no retention period included in the GDPR. Data may be retained no longer than is necessary for the purpose for which they were collected.

The GDPR obliges us to document all data leaks concerning Personal Data. Proper log files are needed to comply with this obligation to document. The Dutch Data Protection Authority may also request this information. The retention period must be long enough for this.

.

is damaging Erasmus MC's interests, or if there is another reason, unrelated to the non-personal monitoring referred to in the previous article, to believe or other concrete facts or circumstances that an Employee is not complying with the Code of Conduct and/or is damaging Erasmus MC's interests, a personal audit of email communication, network traffic or internet use by individual Employees, as part of an investigation into a breach of duty, may be performed by CERT and/or the Audit unit. A written report of this audit will be drawn up.

The following procedure will apply:

- The Executive Board, the Audit manager or the manager of the department where the Employee, who might be guilty of a breach of duty, works, requests an investigation into the email communication, network traffic or internet use of the Employee. An employment lawyer is notified.
- CERT and/or the Audit unit will submit the written report to the Executive Board, the Audit manager or the Employee's manager.
- Having regard to possible personnel consequences, an employment lawyer will be involved at the earliest possible opportunity.
- The collected data will only be used to investigate the alleged breach of duty and for any decisions following on from the investigation.

9.3 If the written report referred to in the previous paragraphs does not lead to further actions it will be destroyed within 1 month.

9.4 The Employee is immediately informed that an investigation is being initiated. This may be deviated from if it is in the interest of the investigation. In that case, the chairman of the Works Council will be informed in confidence.

9.5 Employees working in a confidential position, such as company doctors, confidential counsellors and the mediator, are in principle exempted from personal audit by virtue of their confidential position. This does not apply to checking the security of email traffic.

9.6 Members of the Works Council or Departmental Committees are in principle exempted from personal audit by virtue of the performance of their duties as members of the Works Council or Departmental Committee.
This does not apply to checking the security of email traffic.

10. Operational Management

10.1 In the event of established incidents or established security incidents, the Operator may deny Employees access (temporarily or otherwise) to computers and/or networks.

10.2 Contrary to the provisions of article 4.1, an Employee's mailbox may, with his permission, be transferred to or shared with another Employee. If the Employee in question is not available and the work duties require immediate access, the Operator may provide access to this Employee's mailbox to the manager or a person designated for this purpose by the manager.
This situation only arises if the Employee cannot or will not give permission and there are no other options available to quickly obtain the information contained in the email for work purposes. The Employee in question will be informed of this immediately. The manager or other designated person may not access emails which seem to be private or were sent to or received from a mediator, confidential counsellor or company doctor.

10.3 The Operator is entitled to copy, move or destroy emails or remove email attachments intended for Employees, if this is required for security purposes or the continuity of email traffic. The Employee in question will be informed of this immediately.

10.4 A regular survey of the equipment connected to the network and of the software is part of the operational management of the Internet and ICT Facilities. The data collected during this process will be recorded by the Operator and will only be used for the operational management of the Internet and ICT Facilities and not for other purposes.

11. Special provisions for the Operator

11.1 The Operator is obliged to treat Confidential Information and Personal Data that he has access to as Operator, in strict confidence. Breach of this obligation may be regarded as a breach of duty. Compliance with this article will be monitored by the Operator's manager, Audit and the CERT.

11.2 The Operator must minimise the activities that require access to Confidential Information or Personal Data of individual Employees.

11.3 The Operators will only access the Employee's accounts or Internet and ICT Facilities when given permission to do so by this Employee. Unauthorised access is only permitted in the event of monitoring as referred to in article 9 or operational management or as referred to in article 10, and will take place on the instructions and under the supervision of CERT and/or Audit.

12. Other provisions

12.1 This Code of Conduct may be supplemented with further provisions or amended by the Executive Board in accordance with the current regulations and after the approval from the Works Council.

12.2 All matters not provided for in this Code of Conduct, will be decided by the Executive Board.

12.3 Where this Code of Conduct is referred to, the "Code of Conduct for the use of Internet and ICT Facilities" [*"de Gedragscode Internet en ICT-faciliteiten"*] is meant.

Drawn up and adopted by the Executive Board on 10 December 2018.