CODE OF CONDUCT FOR INTERNET, EMAIL, DOCUMENT AND COMPUTER USE

ETC Foundation

ETC	Management
Date	16 July 2014
Electronic file name	ETC Code of Conduct for Internet, Email, Document and Computer Use

For Approval:

J.H.J. Dusseljee

Director ETC Foundation

TABLE OF CONTENTS

* * *

CODE OF CONDUCT FOR INTERNET, EMAIL, DOCUMENT AND COMPUTER USE

This code of conduct has been compiled in accordance with:

- Article 7:611 and 7:660 of the Civil Code (Burgerlijk Wetboek)
- The Personal Information Protection Act (Wet Bescherming Persoonsgegevens)
- Article 27 section 1 subsections k and l of the Works Council Act (Wet op Ondernemingsraden)

The code takes into account that:

The Foundation and its employees agree to treat each other as a good employer and good employees respectively (art. 7:611BW). The use of the internet and email is indispensable for employees to properly function within the Foundation.

There are risks attached to the use of the internet that make it necessary to set clear rules of conduct. Due to the existence of such risks, employees are expected to act responsibly in using the internet and emailing.

ETC Foundation is entitled to present regulations for the utilisation of the internet and email, and to take measures to ensure the appropriate use of these tools within the institution (article 7:660 BW).

The present code of conduct covering operational procedures and regulations are as follows:

- ETC Foundation is entitled to review personal data for the purposes of monitoring adherence to this code of conduct.
- ETC Foundation emphasises the need to protect the right to privacy and respect the fundamental rights and freedoms of the employees involved when monitoring email and internet use.
- The present code of conduct has been agreed with the support of the Company Council.

In the event of a suspected or proven breach of the code of conduct outlined below, this will be brought to the notice of the Management Team through the line manager involved. The Management Team will subsequently take appropriate action. This may include a penalty proportionate to the severity of the misconduct, and may be anything from a warning to a dismissal.

CODE OF CONDUCT FOR INTERNET AND EMAIL USE

1 SCOPE OF THE CODE OF CONDUCT

This regulation is applicable to all fully or partially automated processing of personal information of those providing services to or employed by ETC Foundation.

2 ASSUMPTIONS

- The monitoring of personal information and data related to email and internet use amounts to the processing of personal data in accordance with the Personal Information Protection Act.
- Any control over email and internet use in ETC must be implemented in conformity with this regulation. Situations not contemplated within the current regulation shall be dealt with in consultation with the selected staff representative and the management team.
- The aspiration is to achieve a good balance between the responsible use of email and internet, and the protection of employees' privacy in the work place.
- The employer will strive to ensure the integrity of the system by providing an internal system manager with external back-up services (referring to the cloud computing arrangement) and the subsequent monitoring this entails.

3 OBJECTIVES

- This code of conduct contains rules to ensure responsible use of email and internet as well as the manner in which control over personal information will take place in relation to email and internet use.
- The monitoring of personal data regarding email and internet use will be put in place in order to:
    a. Provide individual support/review
    b. Avoid negative publicity
    c. Counter sexual intimidation
    d. Guard the company's intellectual property rights and secrets
    e. Ensure system and network security/integrity
    f. Manage costs and capacity
    g. Counter discrimination

4 EMAIL USE

- Employees will be provided with an email support system for their work-related communications. Its use is therefore limited to tasks directly related to each employee's function.
- Limited use of the email system for personal communications is permitted provided this does not disrupt daily proceedings and is not covered by the prohibited activities listed under Article 5.
- ETC recognises that its employees may choose to use their private email addresses for sending or receiving documents when experiencing service disruptions or while abroad on missions. ETC requests

its employees to keep this practice to a minimum and to use only strictly secured and known email addresses for such exceptional circumstances.

5 PROHIBITED EMAIL USE

- Employees are not permitted to use the email system to send or receive messages with pornographic, racist, discriminatory, offensive or inflammatory content, with intimidating (sexual) content or which (could) encourage hate and/or violence, has a threatening content or concerns Spam.
- Employees are not permitted to use the internet system to send or receive chain mail.
- Employees are advised to use only the email programme made available and installed by ETC.
- Employees are advised to use the virus scanner provided to control the integrity of attachments and annexes to an email before opening them.
- Employees are advised to control the integrity of data-ports (USB sticks etc.) before opening them.
- Employees are required to warn the internal system manager if their computer behaves strangely which may signal that a virus has infected the system.

6 INTERNET USE

- An internet system is provided to the employee for work-related use.
- Limited personal use of the internet is permitted provided this does not disrupt daily proceedings and is not covered in the list of prohibited activities enumerated under Article 7.
- ETC recognises that visual and multimedia support is becoming an important tool within the working sphere of its projects and programmes. In such cases, ETC employees can download and save videos, recordings and other such multimedia tools on their computers, but only after having fully verified that this complies with copyright regulations and that the files are virus free.
- ETC recognises that internet-based communication devices are increasingly important and that its employees spend a significant part of their time abroad due to their work. ETC therefore accepts that its employees may utilise online tools to maintain their private lives and personal affairs within reason (i.e. to communicate with family members, listen to music, online banking etc.) or to enjoy their leisure time outside working hours (watching TV and online videos, or listening to music). These activities should be conducted while respecting Article 7, and should not be detrimental to the professional performance of the employee. Moreover, employees are expected to take all reasonable security measures to ensure these activities do not harm or threaten the integrity of electronic documents or computers in their possession.

7 USE OF SOCIAL MEDIA

- Distribution of messages and/or confidential information, regardless of the manner and medium (Facebook, LinkedIn or Twitter, etc.), that could damage the interests of ETC is prohibited. The latter includes any public activity by an employee that could negatively impact on the image of the employer.
- Making public any images, films or other types of information regarding ETC, those involved with ETC (e.g. partners or clients), ETC staff etc. without prior formal permission is not permitted.

- The above does not mean that ETC will not make use of social media as an organisation or through its employees. This is allowed in line with corporate policies and good practice, and is susceptible to the judgement of the Management Team.
- Use of social media for personal reasons only during working hours is not encouraged and is not allowed where it negatively impacts on the duties of the employee.

8 PROHIBITED INTERNET USE

- Employees are not permitted to visit internet sites with pornographic, racist, discriminatory, offensive or inflammatory content. Neither is it permitted to download, reproduce or disseminate such materials.
- The employee is not permitted to procure for him/herself through unlawful access to non-public internet sources.
- Employees are not permitted to download and install illegal software (shareware) from the internet.
- ETC recognises that visual and multimedia support is becoming an important tool within the working sphere of its projects and programmes; and its use and access is permitted in accordance with Article 6.3. However, employees are not permitted to download music or videos from the internet and store these on their work computer utilising illegal software or in conflict with copyright regulations.
- Employees are not permitted to install privately obtained software on ETC-provided computers.
- Employees are not permitted to procure the services of a computer programmer without first requesting consent from the director and the external ICT service provider. Once there is agreement, all licence information will be made available to ETC.
- Employees are not permitted to utilise electronic communication media for unacceptable personal uses. Unacceptable personal use of the internet includes gaming and the downloading of games, gambling or games of chance, pornographic sites, and others covered under Article 8.1.

9 CONDITIONS FOR MONITORING

- Monitoring of personal information through email and internet use will only take place in accordance with the objectives enumerated in Article 3.2.
- In principle, monitoring will takes place at the level of totalised data that cannot be reduced to identifiable individuals.
- In the event that an employee or a group of employees is suspected of contravening the rules, supervision and control measures can be put in place for a short period.
- In principle, monitoring will take place on the level of email traffic and internet use. Only in serious circumstances would monitoring involve the content of these communications and internet use.
- Software-based tools may be utilised to stop prohibited email and internet use. Additional controls may be randomly added.
- If a system manager identifies prohibited use, this will be discussed immediately with the concerned employee. The employee will be informed about the consequences of continuing the aforementioned prohibited use.

10 MONITORING

- Monitoring in the framework of supervision and/or individual assessment will take place at random and will be limited to work-related mail messages.
- Monitoring to avoid negative publicity and sexual intimidation, as well as controls in the framework of system and network security, takes place on the basis of content filtering. Suspicious messages will be automatically returned to the sender.
- Monitoring for leaks of company confidential material will take place randomly on the basis of content filtering. Suspicious messages will be set apart for further inquiry.
- Monitoring regarding costs and capacity management is limited to the internet traffic data.

11 RIGHTS OF THE EMPLOYEE

- ETC will inform its employees in advance of the monitoring of personal data regarding email and internet use, the end goals, the nature of the data, the circumstances under which the data will be obtained and the content of this code.
- Employees can approach ETC to request a full overview of their edited personal data. Such requests will be answered within four weeks.
- Employees can approach ETC with the request to improve, supplement, delete or shield personal data if the material is incorrect, incomplete or not relevant to the case, or contradicts a statutory regulation. Such requests will be answered within four weeks.

12 COMPUTER USE

ETC will provide each employee with a personal computer, either a desktop model for use at the office or a laptop for use at the office, home or during duty-travel. ETC will further provide such accessories that are considered necessary for the fulfilment of the tasks of the employee. All employees receiving any hardware from ETC will sign a contract that describes the conditions for using and preserving the hardware while being employed. This contract is not part of the labour regulations, which refer to a code of conduct only.

- Where there is a problem with the computer, or the presumption of a problem, the employee must contact the internal system manager immediately, who may refer the matter to the external service provider, i.e. the technical firm managing the cloud computing system.
- If there is a presumption of a virus and/or of serious problems, the employee is requested to STOP work and contact the internal system manager immediately.
- When suffering computer problems, the employee is requested to note the following information to help in identifying and then fixing the problem:
    - User name.
    - Date and time when the problem took place.
    - Program in use when the problem took place.
    - Type of error message received (text of the error message if possible / applicable).
    - What you were doing with the programme when the problem presented itself.
    - Which other programmes were also in use at the time of the error.

    - Whether the computer was connected to the internet when the problem occurred.

- Employees are requested to manage passwords in the same way as they would their PIN-code. The computer password is personal and is not to be shared or sent to others.
- When logging in, employees are requested to check if the previous login was made by an unknown person.
- Employees are requested to choose a log-in name and password that they can easily remember and ensure that this cannot be found in a notebook or that it can be easily traced to the employee (therefore, not the name of the employee, a family pet or the children).
- Employees shall NOT use the network password for internet services.
- Employees must NOT write the password on a piece of paper that is posted close to or kept within the computer.
- Employees must NEVER tell their password to others, even to enable use of the computer during absence.
- If an employee suspects that someone knows his/her password, the employee is expected to change it immediately. Employees are expected to contact the internal system manager if they do not know how to change the password.
- Employees should NOT save passwords in their computer. If Windows asks to save a password, the employee is expected to choose “No”.
- Employees should ensure that their password contains at least a number (0 to 9), a capital letter and/or a sign ($, %, &, #, etc.).
- Employees are expected to change their password at least every three months.
- When leaving the room for a lengthy period (e.g. for lunch), the employee is expected to shut the computer down, leave it with a password-activated screensaver, or log out.

13 DOCUMENT USE

- All documents produced by employees are and remain the property of ETC. All documents must be handed over to ETC when employment ceases.
- Documents that are the property of ETC should be worked upon on ETC-owned computers, unless calamity or the unavailability of such tools makes this impossible (e.g. working from home without the availability of an ETC laptop; temporary lack of normal computer due to technical problems). The employee should ensure that all relevant documents that are the property of ETC are stored on the ETC server and easily accessible to all ETC staff.
- Employees should produce and modify all documents according to the ETC house style.
- Employees in possession of an ETC laptop are requested to make regular backup copies of all documents that are the property of ETC by copying the data to the P-file and/or to external devices, such as an external hard disk or USB stick made available by ETC.

14 FINAL DETERMINATION

ETC can modify or withdraw this code of conduct provided it has the consent of the staff representation.