**PROTECT - INTERNAL**

# CCEA Contractor ICT Acceptable Use and Responsibilities

Team Procedure DOFCS/TP/0124/05

***Once printed this version will be uncontrolled. Please refer to the Hub for the current version.***

## Contents



## Document Control

| Date | Version | Update | Author | Reviewer(s) |
|---|---|---|---|---|
| 10/01/14 | 1.00 | Created based on existing informal policy document | Andrew Bruce | Gerry Byrne |
| 26/01/15 | 1.00 | Annual Check – no change | Andrew Bruce | Gerry Byrne |
| 16/12/15 | 1.00 | Annual Check – no change | Andrew Bruce | Gerry Byrne |
| 21/02/17 | 1.00 | Annual Check – no change | Andrew Bruce | Gerry Byrne |
| 21/04/18 | 1.00 | Annual Check – no change | Andrew Bruce | Gerry Byrne |
| 20/09/18 | 3.00 | Template changed. Wording updated on section 10 | Johnathan Cushenan | Gerry Byrne |
| 26-09-19 | 4.00 | Added specific reference to ICT contractors in scope section. | Martin Donnelly | Gerry Byrne |
| June 2020 | 5.00 | BA- new directorate referencing added to procedure | | |
| 30/10/20 | 5.00 | Annual review no change | M Montgomery | M Donnelly |

## 1. Purpose

The purpose of this policy is to provide clarity on what is acceptable use of CCEA-provided ICT services, and the responsibilities that a contractor undertakes when these services are used.

Compliance with the policy is mandatory. Non-compliance with this policy may result in disciplinary action up to and including termination of contract.

Suppliers are responsible for providing their own hardware, software and internet access as outlined in their Contract.

## 2. Scope

This policy covers the following areas:

- Access to Services
- Management of Passwords
- Mobile Working
- Removable Media
- Malicious Software

This policy relates to all Contract for Services Suppliers including:

- Senior Examining and Moderating Teams
- Examiners and Moderators
- Professional Associates (including ICT contractors)

## 3. Access to Services

CCEA provides access to ICT services purely for business purposes. Suppliers must not attempt to access any applications, data, information or other services that are not directly related to their role. Please note the following points:

- Suppliers shall not have access privileges in excess of those required for the efficient conduct of their work for CCEA.
- Suppliers must not make any deliberate attempt to access any data beyond their access privileges.
- Privileges shall be reviewed on a regular basis to ensure that they are still required.
- Each individual user of an information system or computer application will be provided with unique login details (username and password), so that all user actions are accounted for.
- Administrator access to network, operating system, system utility or other high-stakes systems will be provided only to named and qualified parties and permission for this access will be provided in writing.

All access by Suppliers carrying out work for, or on behalf of, the CCEA ICT department will be governed by the CCEA Third Party Access policy and Suppliers may be required to sign a confidentiality agreement.

## 4. Password Policy

Use of passwords is the main information security method used by CCEA and therefore it is essential for all contractors to manage these correctly. The following points form CCEA's policy on password management:

- All workstations in use for CCEA business must be locked with a password if left unattended.
- Passwords must be kept confidential. Even basic access rights may provide a means for a malicious attack to exploit CCEA's systems. Please remember that it is important that no one knows or can guess your password. Treat your password like a bank PIN. Do not tell anyone. Do not 'lend out' your password.
- A password must be changed if compromised.
- A password must not be re-used.
- Any queries about passwords or general computer security issues should in the first instance be referred to the Centre and Examiner Support team.
- Make sure the password you choose can be easily remembered. The first few days after you change your password are when you are likely to forget it. Do NOT ever write down your passwords.
- Users must change passwords every 30 days. Many CCEA systems will prompt the user to do this.

Guidance on password construction is set out below:

### Password recommendations

- Avoid the use of common words.
- Avoid the use of easily guessed passwords such as family names, pets and car registration numbers. Passwords may not contain your username or any part of your full name.
- No blank spaces are allowed.
- Passwords must contain characters from any 3 of the following 4 lists:
    - 0-9 (Numeric)
    - A-Z (Uppercase)
    - a-z (Lowercase)
    - Special keyboard characters e.g. *%£$!&
- Substitute a '5' or a '$' for the letter 'S', or use a numeric '0' instead of the letter 'O', or use '4' instead of 'for', or '2' instead of 'to', etc…
- Passwords must not be less than eight characters long.

## 5. Information Storage

To maintain information systems, and also comply with relevant legislation such as the Data Protection Act, CCEA reserves the right to take appropriate maintenance and security measures. It is, therefore, important that you make note of the following:

- You must not take any action, which may damage the system or service supplied by CCEA or any information/data stored on CCEA systems.
- Information saved on the computer system or service supplied by CCEA is not private. Although it may be invisible to other employees, it can be accessed by authorised CCEA staff.
- Due to rules on data protection you should not store any personal information relating to a living individual other then yourself, or information that is subject to an obligation of confidentiality without proper authority to do so.
- The CCEA network is monitored routinely and all activities are logged and can be investigated should the need arise.
- Sensitive or confidential information in digital form may only be transmitted via CCEA approved systems.

## 6. Use of Personal Computing Devices

- It is the responsibility of a supplier to ensure that specific controls against malicious software are in place e.g. personal firewall, virus scan/protection products.
- It is responsibility of a supplier to make sure that data pertaining to their work for CCEA held on personal computing devices is adequately protected against theft, loss or corruption.

## 7. Equipment

For specific purposes such as Visiting Assessment/Visiting Moderation etc, CCEA may provide equipment that will assist in carrying out the duties of the post. This may include digital recorders, cameras or computing devices and will be provided only where CCEA deems there to be a business need. The use of any CCEA equipment for information storage or processing outside CCEA's premises will be authorised by CCEA under the conditions listed below. Authorisation may be revoked at any time.

- The equipment must be used solely for CCEA business use.
- The supplier shall be fully responsible for the safekeeping and security of any CCEA equipment loaned to him/her.
- The equipment must be protected against theft. For example it must not be left unattended, particularly in public places.
- Manufacturers' instructions for protecting loaned equipment should be observed at all times, e.g. protection against exposure to strong electromagnetic fields.
- All contractors shall return all of the CCEA equipment in their possession upon termination of their contract or immediately on request from CCEA.
- The disposal of CCEA equipment may only be carried out by CCEA.
- No user may install any software onto any CCEA systems or upgrade them in any way.
- Contractors must take great care when downloading or receiving information and files from the Internet to safeguard against both malicious code and also inappropriate material.

## 8. Removable Media (including memory sticks)

Use of removable media is not recommended for CCEA purposes due to the inherent security risks it provides. Where it is used, the following steps must be taken:

- Personal information must not be stored on re-usable media.
- All CCEA-related information on re-usable media must be fully erased so that data may not be recovered before re-use.
- All CCEA-related confidential or sensitive information on re-usable media must be encrypted.
- Non-erasable media containing sensitive or personal information that is no longer required must be provided to CCEA for secure destruction.

## 9. Software Policy

### 9.1 Protection of Copyright

- It is the policy of CCEA to respect all computer software copyrights and adhere to the Terms & Conditions of any licence to which CCEA is a party.
- CCEA will not condone the use of any software that does not have a licence and any supplier found to be using, or in possession of, unlicensed software for CCEA purposes will be considered in breach of contract.
- In relation to work being carried out on behalf of CCEA, all suppliers must ensure compliance with legal restrictions on the use of material in respect of which there may be intellectual property rights, such as copyright, design rights, trademarks. Advice on such restrictions can be sought from the CCEA Business Assurance unit.

## 10. Internet (or Services) Access

Internet access may be granted to suppliers whilst they are on CCEA premises. Authority to use CCEA internet access facilities will be granted on the conditions provided below. Authorisation may be revoked at any time.

- Suppliers must not create, store, transmit or download any material that is illegal, defamatory or infringes copyright, trademark or patent laws.
- Suppliers must not use any CCEA system to distribute unsolicited advertising.
- Suppliers must not use any CCEA facility to send or circulate any text, file, picture, graphic, sound clip or video clip that has the potential to give cause for offence or hurt to feelings to the recipient/s either inside or outside CCEA.
- Suppliers must not use CCEA facilities to create, access, display, download, store, or transmit any text, file, picture, graphic, sound clip or video clip that exceeds the bounds of generally accepted standards of decency and good taste.
- Suppliers must not use CCEA facilities to create, access, display, download, store, or transmit any text, file, picture, graphic, sound clip or video clip that pertains to any product or service not permitted to minors by law.
- Suppliers must not use CCEA facilities to create, access, display, download, store, or transmit any excessively large document, file, picture, graphic, sound clip or video clip such

that this impacts negatively on the performance of CCEA's electronic communications infrastructure.

- Suppliers must not use CCEA facilities to engage in any unlawful activities or any other activities that would bring disrepute on the organisation.
- Suppliers must not use CCEA facilities to engage in personal business and/or commercial activities on the Internet, including offering services or merchandise for sale. .
- Suppliers must not use CCEA facilities to engage in any activity, which would compromise the security of any CCEA computing resources.
- Suppliers must not use CCEA facilities to engage in any unapproved fund raising activity, endorse any product or service, participate in any lobbying activity, or engage in any political activity.
- Suppliers, when accessing and using Internet services through CCEA resources, must ensure that they do not irresponsibly consume resources/bandwidth. Where the download and/or transmission of large amounts of data is legitimately required then technical advice should be sought from the CCEA Information and Communications Technology function.

## 11. Reporting Responsibilities – Security Incidents

All potential, perceived or actual security incidents must be reported immediately to CCEA through the Centre and Examiner Support team. Information Security incidents are events that have impacted, or have the potential to negatively impact on the confidentiality, integrity or availability of CCEA data or information. Security incidents may include software malfunctions on CCEA equipment or those that may impact or actually have impacted on CCEA data/information.