CCFSA CLIMATE CHANGE AND FOOD SECURITY ASSOCIATION

Internet and Email Policy

https://iklimvegida.org.tr/ info@iklimvegida.org.tr

INTERNET AND EMAIL POLICY

Member:	• all board members/trustees, board committee members • all association employees, secondees, interns and volunteers; and • all consultants/contractors/suppliers (including internal consultants with an association email address) • all association partners
Title:	Internet and Email Policy
Document type:	Policy
Date/version:	September 2024 / Version 1
Classification:	General Distribution
Author:	Adil Murat Vural, Head of Management Board
Owned by:	Management Board
Reviewed and approved by:	Management Board
Next review date:	September 2025

1. INTRODUCTION

The Climate Change and Food Security Association (CCFSA)

This policy applies to the Climate Change and Food Security Association, hereafter referred to as 'the CCFSA'.

Many information systems are now electronic and the internet and email are essential business tools. CCFSA staff are required to use them in a competent, responsible, effective and lawful manner. Information created or stored within the organisation's email system constitutes an organisational record. Emails have the same status as any other form of the organisation's business correspondence or written communication and may be subject to disclosure under Data Protection Legislation or Freedom of Information Act (2000).

Staff are granted access to email and the internet for CCFSA business use and for work-related educational and research purposes. Access for limited appropriate personal use in their own time is allowed with their line manager's permission. Staff are also permitted to use personal devices to access staff Wi-Fi in their own time.

2. PURPOSE

The purpose of this policy is to ensure that all CCFSA staff understand their responsibilities for correctly accessing the internet and understand what the organisation deems to be acceptable use of the email system via the organisation's IT systems, while on CCFSA premises, working remotely and when acting in representation of the organisation.

3. SCOPE

This policy applies to all CCFSA staff. For the purpose of this and all other information governance policies, the term 'CCFSA staff' refers to the CCFSA employees, appointees, temporary staff, contractors/agency staff, consultants, students and other individuals working on behalf of the CCFSA.

Failure by any member of CCFSA staff to adhere to this policy and all appropriate supporting guidance will be considered gross misconduct and may result in disciplinary action.

4. DEFINITIONS

Attachment A file attached to an email message, which can contain malicious software and should be opened with care.

Browser The CCFSA uses Microsoft Internet Explorer and Chrome as its standard browsers. NHIS will ensure that the current recommended version is available on all devices that access the internet.

Bandwidth The overall capacity of a network connection/the amount of data that passes through a network connection over time. The greater the capacity, the more likely that better performance will result.

Email system Any computer software application that allows email - message, image, form, attachment, data - to be communicated from one computing system to another.

Information asset Any data, information, information system, computer or programme of value to the organisation's business.

Information sharing protocols Written agreements made within the existing legislative framework between the CCFSA and named organisations to allow sharing of personal confidential data for health and social care purposes.

Internet (World Wide Web) A global system connecting computers and computer networks. For the purposes of this document, the term internet will also encompass the organisation's intranet.

Junk mail Unsolicited email messages usually of a commercial nature, chain letters or other unsolicited mass-mailings (see also **spam**).

Malicious software/Malware Software designed to harm a computer or network. Includes but is not limited to:

• **Viruses -** unauthorised computer code attached to a computer programme which secretly copies itself using shared discs or network connections - can destroy information or make a computer inoperable.

• **Trojan horses -** malicious, security-breaking programs disguised as something benign such as a screen saver or game.

• **Worms** - which launch an application that destroys information on a computer and sends a copy of the virus to everyone in the computer's email address book).

• **Ransomware** - a growing threat in the cyber threat landscape. Usually delivered via phishing emails, which use social engineering techniques (i.e. an email made to look like its sent from a person/name know to the victim or disguised to look like it is from your bank, post office, police etc.) to convince a victim to click a link, download or open an attachment. Once the victim's computer is infected with ransomware, the malicious code will begin to encrypt files on the device (and network), rendering them inaccessible before demanding payment, often in the form of crypto currency such as bitcoin, in return for the ability to unlock that data with an encryption key. Effectively this tactic denies the victim access to their data unless they pay the ransom, or have the ability to restore data from unaffected back-ups.

Personal Confidential Data (PCD) This term describes personal information about identified or identifiable individuals, which should be kept private or secret. For the purposes of this policy 'personal' includes the Data Protection Legislation definition of personal data, but it is adapted to include deceased as well as living people and 'confidential' includes both information 'given in confidence' and 'that which is owed a duty of confidence' and is adapted to include 'sensitive' as defined in the Data Protection Act. This excludes the names of staff, their job role and work location, but does apply to their personal data such as home address, date of birth, financial and HR information.

Personal Data (as defined by Data Protection Legislation) Any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

Phishing Sending an email to a user falsely claiming to be an established legitimate enterprise in an attempt to defraud the user into surrendering private information that will be used for identity theft. The email directs the user to visit a website where they are asked to update personal information, such as passwords, credit/debit card numbers and bank account numbers that the legitimate organisation already has. The website, however, is bogus and set up only to steal the user's information (see also **spoofing**).

Proxy website A server (a computer system or an application) that acts as an intermediary for requests from clients seeking resources from other servers.

Social media For the purpose of this and other relevant information governance policies the term social media includes, but is not limited to, websites and applications that enable users to create and share content or to participate in social networking, blogging, tweeting or social engineering.

Spam Unsolicited email messages, usually of a commercial nature sent to a large number of recipients. Also refers to inappropriate promotional or commercial postings to discussion groups or bulletin boards.

Spoofing Forgery of an email so that it appears to have been sent by someone other than the sender.

User/authorised user An individual given access to the CCFSA's network to access the internet and email.

Wi-Fi A mechanism for wirelessly connecting electronic devices through a network access point.

5. ACCESS

All CCFSA staff requiring computer access will be allocated a network account, email address and access to the internet, following authorisation by an appropriate senior manager. This allows users to log onto a computer, access their email account and utilise the web browser. These services are not available without a username and password. Access to the internet through proxy websites or other methods of bypassing security controls or circumventing internet filtering to access content otherwise blocked is **not** permitted.

Members of the public are **not** permitted to access the internet via a computer connected to the organisation's network or through a Wi-Fi connection. Any user who requires temporary exemption from any part of this policy to access specific information for legitimate work or research purposes is required to obtain written authorisation from the management board.

Users suspected of breaching of this policy may have their access rights suspended until an investigation and any disciplinary procedures have been completed.

6. STAFF RESPONSIBILITIES

Staff using the internet and email must conduct themselves in accordance with their terms and conditions of employment or appointment. Staff must only use the Web Browsers supplied and maintained by CCFSA. Staff must not continue to use an item of networking software or hardware, following a request from a CCFSA manager to cease doing so on the grounds of causing disruption or risk to the correct functioning of the organisation's information systems. Internet monitoring software is in use which records, prevents access to or warns users about certain categories of sites. Where a user has a legitimate business need to access a restricted site they should complete the online approval form for Access to Blocked Internet Sites. It is recognised that in the course of their work or associated research, some staff may have a requirement to access, transmit or receive material that may be defined as offensive, obscene, indecent or similar. In most cases, such internet sites will be blocked and will require unblocking using the Approval Form for Access to Blocked Internet Sites. Access to pornographic images is deemed to be misuse. Where files downloaded it is the staff member's responsibility to obey any licensing terms that may apply.

Staff must obtain appropriate authorisation for any use of Cloud Computing services and should refer to the 'Using the Cloud' Staff Procedure for further information. Downloading images, MP3 files and streaming video or audio can have a significant impact on the performance of the network and must be restricted to authorised business needs only.

Staff are expected to use the same personal and professional courtesy in emails as they would in any other forms of communication. Email messages are written documents and may be used as such in a court of law. They may also be disclosed to the public as the result of a Freedom of Information request. Therefore, staff are advised to create all email messages with a view to them being public correspondence.

Where email is used to communicate externally, users must not give the impression that their personal comments represent the views of the CCFSA unless specifically authorised to do so. The use of email for critical correspondence should not be relied upon without independent verification of receipt. Email addresses are traceable and identifiable to the organisation and usually to individuals. Any comments made on external websites should contain an appropriate disclaimer that is recommended by the CCFSA's Communications Team. Users must also log-in under the standard default setting, which does not allow any attachments to be downloaded or any content to be cached.

7. PERSONAL USE

Access to email and the internet is provided to staff for CCFSA business-related purposes, but it is accepted that they may be accessed for purposes not directly relevant to the organisation's business. This should be limited and reasonable use and only take place outside an individual's normal working hours or during authorised rest periods, with line management direction, and where this does not interfere with the normal work duties of the individual or others. There is no absolute right for staff to use email or internet for personal use. Access to the internet and email that is not for CCFSA business should only take place where it complies with the organisation's view of appropriate use, as indicated by this policy.

Personal emails should be labelled as personal; staff should be aware that personal emails may be accessed under certain circumstances. The CCFSA will not be liable for any financial or material loss to an individual user when using email for personal use. The CCFSA will not be liable for any financial loss to any external supplier of goods and/or services in the event of an individual user failing to honour any financial obligations contracted to that supplier whilst using the CCFSA's email system for personal use.

8. USE OF SOCIAL MEDIA

Access to social media sites is restricted to staff who have a legitimate reason to be provided with access. Only authorised staff are allowed to communicate on behalf of the CCFSA via social media, and the use of the CCFSA's corporate logo or other visible markings or identifications associated with the CCFSA is not permitted. All CCFSA employees and appointees are reminded of the confidentiality statement included in their contract of employment and all staff are reminded of their duty to comply with all information security requirements in the organisation's suite of information governance policies.

Staff must not disclose any CCFSA information that is or may be sensitive, confidential and person-identifiable, or subject to a non-disclosure contract or agreement. 9.5. Staff should not divulge details of their NHS employer on their personal profile pages. If this information is divulged staff must state that they are tweeting/blogging etc in a personal capacity.

9. TRANSFER OF PERSONAL CONFIDENTIAL DATA AND CONFIDENTIAL CORPORATE INFORMATION

All transfers of personal confidential data must comply with Data Protection legislation and Caldicott Principles. In particular, they should:

• Be an approved lawful data flow agreed by the SIRO and DPO.

• Be notified to the Information Governance Team to record on the Data Flow

Mapping register.

• Only be sent on a 'need to know' basis.

• Be supported by a justifiable reason to send the information.

• Be pseudonymised, wherever possible.

• Be sent using adequate security as per local and national guidelines.

The principles of confidentiality and data protection must also be applied to the email transfer of information associated with confidential corporate information. Individual users are prohibited from using instant messaging services such as, but not limited to, Microsoft Messenger or Yahoo Messenger. Individual users must NOT send or forward PCD or CCFSA commercially sensitive data to personal non-work email addresses. Examples include but are not limited to Google/Gmail, Hotmail, Yahoo mail, AOL mail, internet or remote storage areas and email services provided by other ISPs. Agreed information sharing protocols must be in place when regularly sending or forwarding PCD to individuals in other organisations. PCD or CCFSA commercially sensitive data should only be exchanged electronically when encrypted to at least the minimum-security standards.

10. EMAIL RETENTION AND DELETION

Attachments and emails should be saved to an appropriate directory on the shared network drives. Information must not be saved onto the C:Drive or desktop unless this is on an **encrypted** laptop and access to the network is unavailable. The email system should not be used as a general repository for records. Emails and their content may be classed as a corporate record and therefore could be requested under the Freedom of Information Act (2000) and the Data Protection legislation. This applies to all retained emails (including those held in 'deleted Items' and email folders), regardless of their content, sender, whether they relate to the business of the organisation, service users, members of the public, or have been generated by staff for purposes not directly relevant to the CCFSA.

11. PROTECTION AGAINST VIRUSES

All computer equipment within the CCFSA is virus protected, and incoming messages are virus checked. However, users should report any unusual occurrences relating to the performance of their computer to the IT Service Desk.

12. INCIDENT REPORTING

All actual, potential or suspected incidents involving use of email or internet need to be documented in line with the CCFSA's Incident Reporting Policy. Incidents may need to be

entered on the Incident reporting module of the Data Security and Protection Toolkit. These will usually be incidents where there is a loss of personal data involving a large amount of individuals or particularly sensitive personal and confidential information has been disclosed without the legal basis to done so or in error.

13. MISUSE OF THE INTERNET AND EMAIL SYSTEMS

Misuse of the internet or email system may make both the user and the CCFSA liable under law, or may impede the function of the CCFSA's network systems and affect wider network users and the efficient functioning of email. All users are responsible for complying with the 'Personal Use' and 'User Responsibilities' sections above and for ensuring that they do not use the CCFSA's email and internet system for:

a) Accessing, composing or transmitting any material considered to be illegal, racist, homophobic, immoral, offensive, obscene, libellous, defamatory, harassing or pornographic (other than for lawful and properly supervised purposes – see section 7.7 above).

b) Accessing or transmitting pornographic images falling into the following categories:

• Level 1: Adult images;

• Level 2: Explicit images;

• Level 3: Illegal images.

Instances where Level 3 images are involved will be reported to the police.

c) Transmitting material that incites others to criminal, racist, homophobic or terrorist acts or incites them to contemplate such acts.

d) Creating or transmitting defamatory material (note that common law and statutes pertaining to libel apply to the use of the internet) regarding the CCFSA, CCFSA business, service-users or staff.

e) Creating or transmitting material designed to or likely to cause annoyance, inconvenience or needless anxiety to service users, other CCFSA staff or the general public.

f) Downloading or distributing 'pirated' software.

g) Transmitting unsolicited commercial or advertising material to other users, organisations.

h) Deliberate corruption or destruction of other users' data or work.

i) Accessing and using other staff member's email account without their permission or any other deliberate violation of another user's privacy.

j) Undertaking activities that deny service to other staff members e.g. accessing streaming video for non-work purposes, sending unwarranted global emails or excessively large emails.

k) Any deliberate attempt to disable, defeat or circumvent the organisation's internet firewall and other security measures in place to protect the network.

l) Downloading any shareware or freeware without authorisation by CCFSA.

m) Undertaking activities for personal or commercial financial gain (e.g. sales of personal property, gambling or share dealing) or for political lobbying.

n) Forging or attempting to forge email messages (e.g. spoofing).

o) Streaming of video or audio for personal use without permission.

14. INVESTIGATION OF SUSPECTED MISUSE

Any suspected misuse of the internet or email system identified through routine monitoring procedures will initially be attributed to, and be the responsibility of, the associated logged-in user. Where inappropriate use is suspected from the results of routine monitoring or identified through other incidental management board will be informed. Where any breach of this policy has been established, appropriate action will be taken in accordance with the CCFSA's Disciplinary Policy.

15. MONITORING OF INTERNET AND EMAIL USAGE

Monitoring records will be maintained by CCFSA, audited periodically and only communicated to those with a valid need to know. If a user inadvertently accesses a site to which they believe access should be prevented they should immediately inform the management board.

16. EQUALITY AND DIVERSITY STATEMENT

The CCFSA is committed to ensuring that the way we provide services to the public and the experiences of our staff does not discriminate against any individuals or groups on the basis of their age, disability, gender identity (trans, non-binary), marriage or civil partnership status, pregnancy or maternity, race, religion or belief, gender or sexual orientation. As an employer, we are committed to promoting equality of opportunity in recruitment, training and career progression and to valuing and increasing diversity within our workforce.

To help ensure that these commitments are embedded in our day-to-day working practices, an Equality Impact Assessment has been completed for, and is attached to, this policy.

17. COMMUNICATION, MONITORING AND REVIEW

The CCFSA will ensure that the policy is circulated to the policy 'audience' as documented in the control section of this document. Also ensuring that any key changes to the policy are highlighted. This policy will be monitored by the Information Governance team through the review of incident reports where staff are found to have sent information inappropriately or erroneously. The CCFSA will also check staff awareness of phishing emails by sending out a test phishing email. The results of the exercise will inform staff communications, IG Training and awareness activities and may also result in staff being approached at an individual level to undertake further training.

18. STAFF TRAINING

The policy will be highlighted to staff upon their induction to the CCFSA. Any individual who has queries regarding the content of this policy, or has difficulty understanding how this policy relates to their role, should contact the management board.