Email Policy (External)

Information Services (IS)

Cranfield University respects that all users have a right to privacy but retains the right to monitor and access all information on University IT systems to safeguard data and ensure compliance with Janet[1] network provisioning, University policies and all other applicable legislation.

This policy outlines how email shall be used by users of the University's IT systems, but as email cannot be considered secure further measures should be taken to protect sensitive personal or confidential information.

1. General

It is important that users do not intentionally participate in the creation or transmission of any obscene, defamatory, harassing (including through language, frequency or size of messages), threatening or otherwise inappropriate and/or illegal material. They shall also take reasonable steps to prevent unauthorised use of their accounts including:

- keeping their passwords secure,
- being aware that email is a likely channel for the receipt of malicious links and attachments,
- not responding to requests to enter user credentials in untrusted/unknown sites or portals
- reporting any suspicious emails through 'abuse@cranfield.ac.uk'.

Users shall not participate in the sending of unsolicited email, including hosting or allowing the hosting of sites or information that are advertised as such from a third party network or supplier. Where there is a justifiable business reason for sending commercial or bulk email, then this should take place using trusted mailing lists and be in full compliance with the Data Protection Act and General Data Protection Regulation. The use of email addresses and groups is further covered in the Email Guidelines document and a number of internal groups have been created to facilitate the dissemination of information to subsets of users (for example staff/ students/researchers attached to individual Schools/Professional Service Units).

Where emails contain information of a contractual or legal nature these need to be retained for the same number of years as those that apply to printed materials to meet statutory or contractual requirements.

Special care and security considerations are required when sending confidential or sensitive personal data in attachments and they shall be password protected as a minimum, but further advice can be found in the University's Information Handling Procedures.

Also, users shall not construct, alter and/or forge headers of email messages to fraudulently mislead other users or to prevent them from responding to messages, and they must always be careful to ensure that email is only sent to the intended recipient(s).

[1] Network specifically for the UK research and education community -https://www.jisc.ac.uk/janet

2. Account management

If a user is unexpectedly absent for a prolonged period, then permission may be sought by the line manager/supervisor to access the person's email. All such requests shall be authorised by the requesting person's Line Manager and will only be granted where there is a legal or specific business requirement to undertake such access, as per the 'Access to Electronic Information' standard procedure, which can be found at the following location: https://intranet.cranfield.ac.uk/it/PoliciesandProcedures/Access_to_Electronic_Information.pdf

Staff accounts will ordinarily be closed upon leaving employment with the University resulting in the cessation of the email address and the general unavailability of the account contents. Where there is a legitimate need (University and/or legislative purpose) access to the account can be authorised for a strictly limited period of time. All ex-staff email mailboxes will be held for a maximum of 1 year before being deleted.

If requested by the user's line manager an external message can be activated to automatically 'bounce' messages to any sender, but this will only provide alternative details of a Cranfield University contact point.

If there is a requirement to continue receiving internal Cranfield email, arrangements can be made to either continue forwarding these to the existing email account, or to an alternative email account but this will only take place for a limited time on the approval of a Pro-Vice Chancellor of a School or Service Director of a Professional Services Unit.

Staff shall seek approval from the Director of Information Services prior to automatically forwarding University emails to third party email systems, and specific checks will be taken to ensure that this is complied with.

If there is a requirement to disable an account this can be undertaken on the authority of any member of the Senior Management Team but any such actions must be justified and auditable to ensure that relevant processes are followed.

3. Use of generic email addresses/accounts

Generic email aliases must be specific to the faculty/department. Generic emails such as info@cranfield.ac.uk shall not be given to an individual school unless there is no possibility of the word being needed by any other School or Professional Service Unit (PSU) in the future. In addition, thought should be given when devising the email address so that it is easy for the end-user to remember and type accurately.

In all cases any requests for generic email addresses must be submitted to Communications and External Affairs PSU who have to approve their creation before any literature or advertising is commissioned.

Details of the generic email address should be forwarded to the IT Service Desk so that it can be included in the email address directory and, where it is to be used for promotion, a generic email address should always be used in preference to a personal one.

Generic email addresses should be accessible to at least two members of staff; individuals will not be allocated a generic address. This helps to guarantee a prompt and effective response. Any changes to users of the email address, including when applicable staff leave, should be reported to the IT Service Desk so that the information relating to the email address can be updated.

4. Additional policy for Cranfield Defence and Security (CDS) staff/PhD students

Staff and PhD students at CDS (Shrivenham) are also allocated an email account on the Defence Academy system (<forename>.<surname>@defenceacademy.mod.uk). This account is managed on behalf of the Defence Academy by its Campus Integrator contractor, and rules for its use are set by the Defence Academy.

All Not Protectively Marked (NPM) email communications by CDS staff should normally be transmitted via the Cranfield email system (@cranfield.ac.uk).

OFFICIAL-SENSITIVE information may be transmitted either within the Defence Academy (DA) via Defence Academy email, or via MoD's DII(F) for transmission to members of the wider MoD community. *Any such emails and/or attachments shall not be sent or forwarded to any external email address, or saved to any storage facility other than the approved storage facility on the Defence Academy Network.*

All CDS staff are required to check DA email regularly when on site and to post a suitable 'out of-office' message when working off site.

All CDS staff are expected to check their Cranfield email daily while on campus; when working remotely they should check their email as regularly as possible.

5. Disclaimer

The following disclaimer should be added to all out-going email sent from any University system or address: -

"This email and any attachments to it may be confidential and are intended only for the named addressee. If you are not the named addressee, please accept our apology, notify the sender immediately and then delete the email. We request that you do not disclose, use, copy or distribute any information within it.

Any opinions expressed are not necessarily the corporate view of Cranfield University. This email is not intended to be contractually binding unless specifically stated and the sender is an authorised University signatory.

Whilst we have taken steps to ensure that this email and all attachments are free from any virus, we advise that, in keeping with good computing practice, the recipient should ensure they are actually virus free."

6. Relevant legislation, enforcement and operation of policy

Under the Telecommunications (Lawful Business Practice [LBP]) (Interception of Communications) Regulations 2000 (Statutory Instrument 2000 No.2699) the University reserves the rights to monitor users' activities to:
- record evidence of official transactions;
- ensure compliance with regulatory or self-regulatory guidelines;
- maintain effective operations of systems (e.g. preventing viruses);
- prevent or detecting criminal activity;
- prevent the unauthorised use of computer and telephone systems (i.e. ensuring that the users do not break the law or breach university policies).

In addition, the Freedom of Information Act, Data Protection Act and General Data Protection Regulation place obligations on the University in releasing information when requested to do so, and it is imperative that all users understand the consequences and possible repercussions of this when compiling email messages.

Although the university policy is that IT staff will not actively spend time looking for computer misuse, the Information Services PSU will investigate issues once made aware of them or when they are discovered in carrying out normal service operations or audits.

IT PSU administrators do not routinely check contents of email, and will only review the contents of emails if they receive a request from the user(s) of the mailbox or through an authorised request (as per the 'Access to Electronic Information' process) from the Director of IS, Director of Human Resources & Organisational Development, Data Protection Officer or the Academic Registrar to make these emails available for appropriate investigations.

There are certain circumstances where header information may be viewed and/or examined by the email administrators to resolve technical issues, such as log analysis or determining suspected spam emails, but this information shall always be treated as being private and confidential.

Where the IT Service Desk receives a complaint from recipients or other third parties regarding a mailing, or any mailing causes technical problems on the University's email systems action may be taken to stop the mailing immediately or prevent it reoccurring. This may result in the suspension/termination of the sender's account(s) and could happen without warning or notice.

Failure to comply with this policy may lead to disciplinary action.

Document control

Document title	Email Policy (External)
Originator name/document owner	Information Security
Professional Service Unit/Department	Information Services
Approval by and date	Information Assurance Committee; 21/09/2021
Date of last review and version number	September 2021; V1.7
Date of next review	August 2020
Information categorisation	Open

Document Review

Version	Amendment	By	Date
1.5	Added “safeguard data” to opening paragraph + date changes	Information Security	September 2019
1.6	Date and numbering changes only	Information Security	September 2020
1.6	Date and numbering changes only	Information Security	September 2021