# ISC10D029

## Security Procedure SP1 – Communicating Passwords to Users

This document details basic procedures that should be followed when communicating passwords to users, either to new users, or when dealing with incidents where a password change has been required and this needs to be communicated to the user.

- Only those staff authorised to do so should communicate passwords to users. For Information Service managed IT accounts, such as the UEA IT account allocated to all staff and students, only IT Helpdesk staff should inform users of their password following separate additional detailed procedures documented in Helpdesk operational documents[1].
- Other staff authorised to inform users of passwords, such as departmental IT support staff allocating passwords for accessing local IT resources where authentication is not controlled by centrally managed Active Directory processes, or course administrators who have been allocated a batch of visitor IT accounts by Information Services for distribution to attendees, should follow the procedures below.
    - Wherever possible the user should be informed of the password by face to face contact. Before informing the user of the password, their identity should be checked[2].
    - Where face to face contact is not possible, the user's password should be communicated to them over the telephone after asking them to confirm their full name and at least one other piece of information that has previously been collected as part of the authorisation process(e.g. date of birth).
    - The password should be communicated to no other person other than the user, and the user should be reminded that they must keep the password secure and must not under any circumstances disclose it to any other person.
    - Wherever possible the resource/facility being accessed should be configured to force a change of password when the user first accesses the resource/facility[3] . If this is not possible/practical, they should be instructed to change the password at the first opportunity.
    - Passwords should never be sent via email to recipients.

[1] Helpdesk operational documents are stored on the ISD intranet with access restricted to the Helpdesk and other authorised Information Services staff.

[2] Where the user has been allocated a campus card they can be checked against the photo on the card.

[3] Enforcing a change of password when first accessing the facility will depend on the type of facility being accessed.