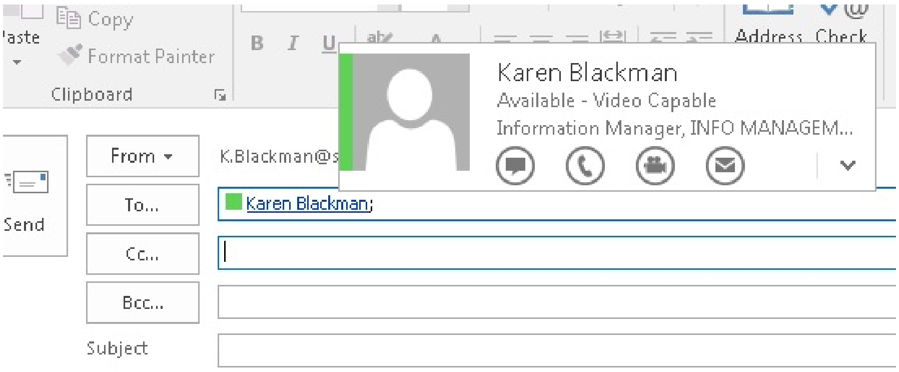
Auto-complete

Auto-complete is the tool within Outlook which displays names and email addresses as you start to type them, offering possible matches based on names and email addresses gathered from the emails that you have sent in the past. Using this feature can save time, but it can also lead to emails being sent to the wrong people – for instance, where you have regular contact with two staff members with similar names or a student and staff member with similar names.

If using auto-complete, then names should always be double-checked before emails are sent; you can also ensure that recipients are correct by hovering over them within Outlook, which will show the person's job title and team/department/area:

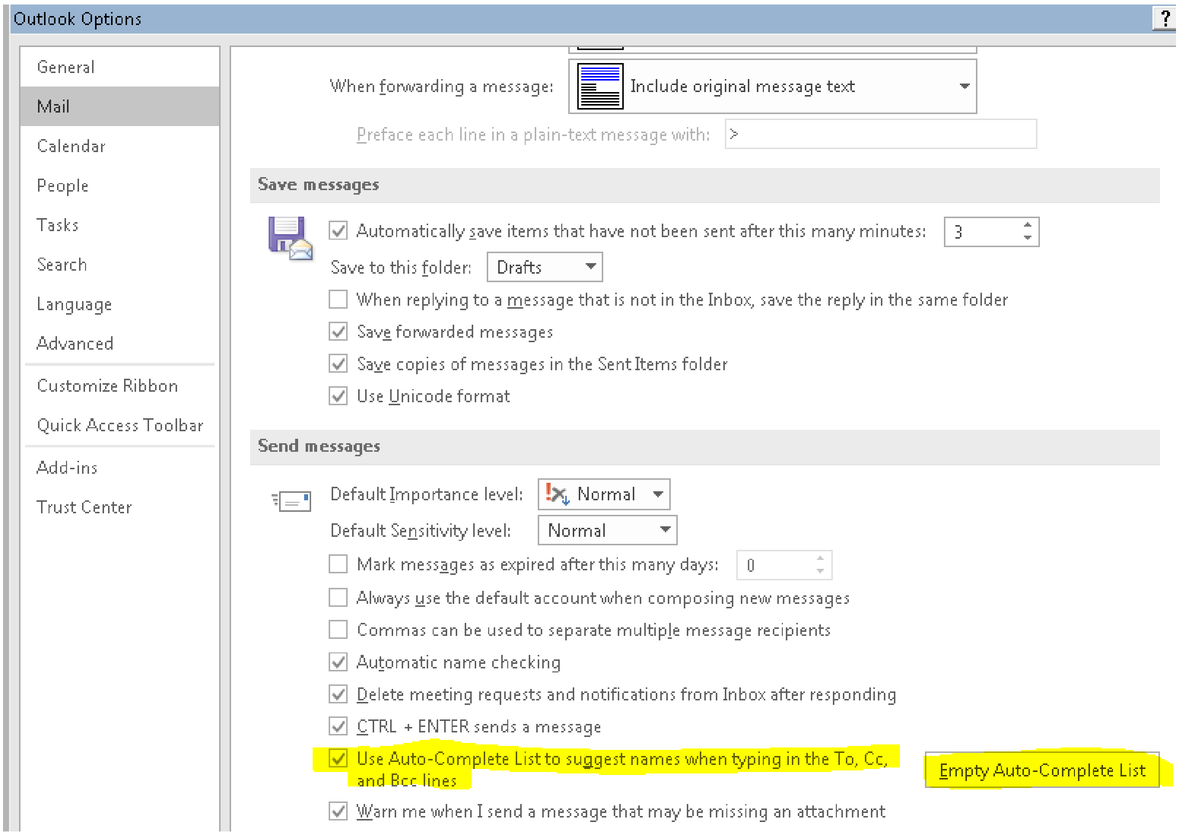


Karen Blackman
Available - Video Capable
Information Manager, INFO MANAGEM...

From: K.Blackman@s

To: 🟩 Karen Blackman;

To mitigate the risk of a breach, you can disable the auto-complete function within Outlook, by clicking on 'File' then 'Options' and unticking the relevant box (you can also clear existing auto complete options as an alternative measure in the same place):



When forwarding a message: Include original message text

Preface each line in a plain-text message with: >

Save messages

☑ Automatically save items that have not been sent after this many minutes: 3

Save to this folder: Drafts

☐ When replying to a message that is not in the Inbox, save the reply in the same folder

☑ Save forwarded messages

☑ Save copies of messages in the Sent Items folder

☑ Use Unicode format

Send messages

Default Importance level: Normal

Default Sensitivity level: Normal

☐ Mark messages as expired after this many days: 0

☐ Always use the default account when composing new messages

☐ Commas can be used to separate multiple message recipients

☑ Automatic name checking

☑ Delete meeting requests and notifications from Inbox after responding

☑ CTRL + ENTER sends a message

☑ Use Auto-Complete List to suggest names when typing in the To, Cc, and Bcc lines

Empty Auto-Complete List

☑ Warn me when I send a message that may be missing an attachment

Replying to or forwarding chains / ‘reply all’

You should pay close attention when replying to or forwarding email chains or using the ‘reply all’ function, as this can often lead to an inadvertent personal data breach.

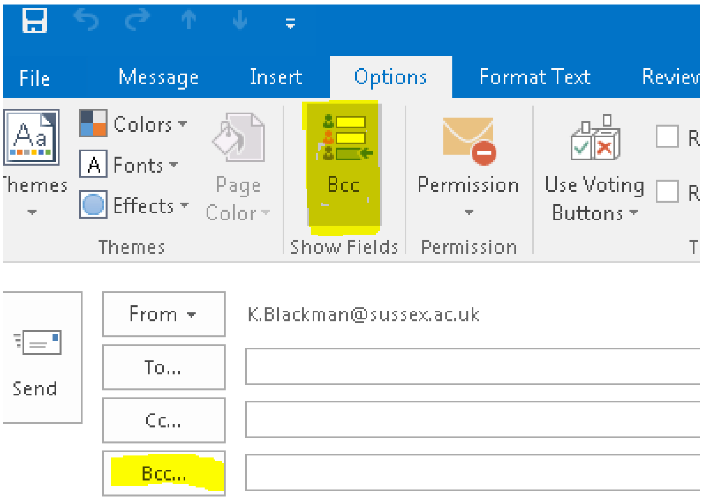
If forwarding to or including a new recipient, ensure that any personal data included within the existing chain is something that they are authorised to access, and that it is necessary for them to see, particularly if the new recipient is an external contact.

The same applies if you are replying to an email including multiple recipients; if you are using the ‘reply all’ function, particularly if you are adding any additional personal data to the chain in your response, you should ensure that all recipients are authorised / required to have access to the data.

Using ‘cc’ vs ‘bcc’

When copying an email to a number of individuals, it is important to consider whether the copy (‘cc’) or blind copy (‘bcc’) function should be used.

The ‘bcc’ function will ensure that the email addresses and names of the individuals you are contacting are not visible to other recipients. If the ‘bcc’ field does not appear as default in your email, this can be added via the options tab within an email – please see the below screenshot for reference:



K.Blackman@sussex.ac.uk

Whilst it may be appropriate to use the ‘cc’ function for an email conversation on a particular matter between specific colleagues, or a small group of students who are in a seminar group together and already know each other, blind copy should be used for larger groups and more general communication. For instance, if you are emailing all students on a course or in a particular year, all students who attend a large lecture, or larger groups of staff who are part of a network but are not necessarily known to each other, blind copy is more appropriate and safeguards personal data.

Copy and paste

Whenever using copy and paste in relation to emails (for instance, copying an email address to paste into the ‘to’ field, or copying content from another email or a document to paste into the body of an email), please double-check before sending your email that all information has copied correctly. It is easy to inadvertently send an email to the wrong person when doing this, or to paste the incorrect material into an email and hit send.

Attachments

Attachments can present an additional and heightened risk in terms of personal data breaches originating from emails – for example, if an incorrect attachment containing personal data is included with an email, or if an incorrect recipient has access to an attachment containing personal data.

Please always double-check attachments and recipients before sending. There are also some additional measures that should be considered in relation to attachments:

- Attachments containing a large volume of personal data and/or any amount of special category data*should be password-protected, and the password should be provided separately (either via another email or communicated verbally, e.g. by telephone).

- If sharing documents containing personal data with internal colleagues, you should also consider linking to a secure location that only authorised individuals can access (e.g. a g: drive or Box folder with restricted access) rather than attaching documents to an email, where possible.

Group email lists (e.g. all staff within an area)

When using email mailing lists to send emails (to a group of people) which contain personal data, you should always double-check that you are (a) using the correct list and/or (b) that you are aware of who is included within the list. For example, a Division may have a group email address for all staff in the Division as well as group emails for specific teams or areas of work within the Division. Always make sure you are sending information to the appropriate group email address.

You should also be careful when replying to emails you have received via a mailing list address – for instance, if you click the 'reply all' function to respond to an email you have received because you are included on a mailing list, all individuals also on the list will receive your response. As above, if your response contains personal data, you should be certain that everyone is authorised to access the data and it is appropriate to respond to all.

Contacting students – current/past

To process personal data, we must have a legal basis* for doing so; the legal bases for the University's general business as usual processing are broadly covered off in the University's privacy notice.

There may be some cases, however, when current or former students are being contacted via email by University staff on the basis of legitimate interests (rather than it being necessary as part of our provision of education) – for instance, contacting students from a particular area or cohort, or who were on a module that you have previously taught, about an opportunity or event they may be interested in.

In these cases, it is important to be mindful of data protection principles and data subject rights and ensure that:

- The personal data you are processing is up to date and accurate (e.g. that email addresses are correct; that if correspondence relates only to current students, you are not contacting students who have withdrawn from the University, etc)

- You are clear as to why the individual is receiving communication (for example, by opening your correspondence with a line explaining 'you are receiving this email because…')

- You provide individuals with an opportunity to 'opt out' of receiving future correspondence of the same nature should they wish to, and you must have a mechanism in place for ensuring that they are not contacted again if this is the case, e.g. removing them from your mailing list.

And finally – a note about subject access requests and emails

Individuals have a right to request access to any of their personal data held by the University under data protection legislation. This includes access to emails which identify them and are held on University servers (within your email account and/or deleted items) and within University-held paper and electronic files. This should be kept in mind when using emails for matters which relate to personal data. In light of this, please note the following reminders:

- Don't include anything in an email concerning an individual that you wouldn't want shared with them

- Practice good records management and delete emails that are no longer required

- When deleting emails that you don't need, ensure that you permanently delete your deleted items folder. Alternatively, if you highlight the email in your Inbox and click 'Shift' and 'delete', it will permanently delete the email in one step.

- Only include what is necessary in emails for the purpose in question

More information regarding* ***special category data* *and the* ***legal bases for processing*** *can be found on the University's data protection webpages here.*