Guidance

Data protection information handling - good practice guide

Using Microsoft 365 & Teams securely

- Teams and private chat are persistent (permanent – unless deleted) and are to be treated the same as email – as such, they are recorded information that could potentially be subject to Freedom of Information and GDPR requests.
- Documents and files that you do not wish to keep should be deleted from Teams, Chat and 'Files' regularly to ensure good data housekeeping.
- Stop and consider who you are sharing files with, does it contain sensitive and/or personal information? - are you sharing with a service or third party that would not have permission to see its contents.
- Double-check that you are sending the correct attachments.
- Ensure that all documents are redacted appropriately for the intended recipient.
- When sharing spreadsheets, check for hidden tabs and columns that may contain additional information you do not intend to share.
- Avoid including personal data in the chat heading or text, unless necessary.
- Once completed, documents and files may be stored within MS Teams, but you must consider whether a completed document needs to be moved to the relevant file storage locations/case management files for your service.
- All your actions within Teams and the 365 platform must comply with our Data Protection policy and guidance which can be found at Data protection.
- For more information on how Microsoft 365 & Teams should be used, please consult the full Code of Practice.

Emailing information securely

You should always;

- Stop and consider this guidance before you press 'Send'.
- Restrict the information being sent, and the number of recipients, to the minimum essential for the purpose.
- Ensure you know the identity and right of access of anyone to whom you pass information.
- Double-check all recipient names and email addresses prior to sending an email.

- If you have obtained an email address verbally/by telephone, spell the email address back to the individual who provided it, to verify that you have taken the address down correctly.
- Double-check that you are sending the correct attachments.
- Ensure that all documents are redacted appropriately.
- If attaching spreadsheets, always check for hidden tabs or columns, as these may contain additional information which you do not intend to share.
- When emailing to more than one external recipient, use 'Bcc' at all times, unless there is a legitimate reason why the names and email addresses of recipients would need to be shared with all.
- Adopt a 'peer-checking procedure' whenever sending special category data by email, by asking a colleague to check that you have completed the above actions correctly.
- Avoid including personal data in the subject line, unless necessary.
- Ensure that you know the difference between using an email mailbox and an email distribution list and use each one appropriately.
- If sending special category data / sensitive information via e-mail to a recipient for the first time, send a 'test' e-mail first to ensure you have the correct address.
- Consider using a secure email address (such as GCSX or similar) where sensitive information is being sent and such a facility is available.
- Copy and paste personal data into emails, where possible, rather than risk typing it incorrectly.

When fixing calendar appointments involving external recipients which involves using their personal email address do follow this procedure;

1. In the new meeting request, in the Show group, choose Scheduling Assistant > Add Attendees.
2. In the Resources box, type the name or email address of each person you want to receive a copy of the meeting, but not be listed as an attendee.
3. If you've already added them to the list of attendees, click to the left of their name and choose Resource (Room or Equipment) from the drop-down list.

   Important: This will put the attendee's name in the Location field of the meeting request. To avoid their email address showing up in the location field, change the location venue name before sending

4. Finish filling out the meeting request as you normally would, and choose Send.

[See Microsoft help page for help with setting up a meeting]

You should not;

- Make personal comments in email correspondence (such comments constitute 'personal data' and need to be provided to the data subject if requested) – keep what is said to only what is necessary for the purpose of carrying out the task.
- Forward email chains or "reply to all" unless absolutely essential and only after you are satisfied that all recipients are entitled to all of the information being sent and that there is no inappropriate content.
- Send personal or confidential information by email without first double-checking everything, including recipient names and email address, and all attachments.
- Send a password for a password protected attachment in the same email as the attachment.

Printing Information securely

This guidance covers the correct procedure and additional precautions to take when printing person-identifiable and/or confidential/sensitive information.

You should always:

- use the 'Follow-me' secure release function (where available).
- only print information if absolutely necessary
- check your print settings prior to every print job, to make sure that the correct printer is selected
- check all paper trays are full before beginning your print job
- check all pages are accounted for before leaving the printer
- check your print-outs for cross contamination by users who may not have used the 'Follow-me' secure release print function
- securely dispose of any unwanted or damaged print outs by using the confidential waste bins provided

You should not:

- print personal or sensitive data that is not necessary
- leave the printer unattended whilst printing documents
- leave documents on the printer
- print a colleague's print jobs

Scan information securely

This guidance covers the correct procedure and additional precautions to take when scanning person-identifiable and/or confidential/sensitive information.

You should always:

- scan information in promptly
- use the 'scan to email' function wherever possible
- double-check that you have typed in the email address correctly, before pressing the button to scan
- check the device settings prior to scanning to make sure a previous user's email address is not in the recipient list
- check all pages of the original document are accounted for when leaving (check under the lid)
- securely dispose of any unwanted originals in the confidential waste bins
- if your scanned document does not appear where it should then check with anyone else who may have access to the location to see whether they have moved it and if not, report the details to Strata Helpdesk (01395 517433) who can attempt a recovery.

You should not:

- scan personal or confidential information unnecessarily

- leave the scanner unattended whilst scanning documents
- leave scanned documents on the printer
- leave sensitive or personal data scanned to a shared folder for any length of time, under any circumstance.

Post information securely

This guidance covers the correct procedure and additional precautions to take when sending person-identifiable and/or confidential/sensitive information by post.

You should always:

- if possible, send the information via email instead
- restrict the information to the minimum essential for the purpose
- make sure you know the identity and right of access of the recipient(s)
- include the intended recipient's full name, job title (if applicable) and full address, and then double-check that you have done this correctly
- make sure that all documents are redacted appropriately (if applicable)
- double-check the contents and any enclosures to make sure you are sending the correct information to the correct recipient and address
- if you have obtained an address verbally/by telephone, read the address back (including spellings where appropriate) to the individual who provided it, to verify that it is correct
- clearly mark the envelope 'private and confidential' and/or 'to be opened by addressee only'
- adopt a 'peer-checking procedure' whenever you send special category personal data by post – always ask a colleague to check that you have completed the above actions correctly
- ensure the envelope is properly sealed prior to posting
- include a return address (we suggest a sticker with the words 'If undelivered, please return to:' with the return address, over the flap of the envelope to deter incorrect recipients from opening confidential post received in error)
- if posting a number of documents, count how many letters and envelopes you have at the start and then count again when you are finished – a discrepancy between the two figures will indicate an error
- if the content is highly sensitive, track the delivery of the information by using special delivery by a reliable transport courier (NB: Royal Mail recorded delivery service is not tracked)
- use a method of guaranteed secure delivery if, in exceptional circumstances, manual files or records are required to be sent by post, and always record what information is being sent, why, where, and to whom it is being sent (use a tracer process for manual files)
- only use an encrypted device, if in exceptional circumstances you are required to send electronic information by post and always liaise with Strata before doing this.

You should not:

- send information by post if it is possible to send the information securely by email instead
- send any information unless you are absolutely certain of the recipient's identity and entitlement
- send any information by post without double-checking that you are sending the correct letter with the correct enclosures (where applicable) to the correct recipient, at the correct address

- include a password with an encrypted device sent by post, ask the recipient to contact the sender for the password or send it separately using a method of guaranteed secure delivery and arrange for the recipient to confirm receipt.

Keep my office and workstation secure

The following guidelines should be followed by all employees to help improve the efficiency of their office and workstation and reduce the risk of a security incident occurring.

You should always:

- store information electronically wherever possible
- follow the relevant guidelines for printing / scanning
- lock your computer screen when you leave your desk
- make sure that visitors are accompanied at all times while in the building
- challenge any individual 'tailgate' you as you enter an EDDC building or office, if you don't know their identity
- destroy or dispose of paper files securely; for example, by placing in the confidential waste bins
- keep your desk clear of any papers besides those required at any particular time
- make sure that all storage facilities can be, and are, locked when not being accessed
- make sure that all personal or confidential information held in any form (such as paper, CDs, memory sticks, etc) are locked away when unattended
- make sure that keys to cupboards are stored securely and only accessible to those individuals who require access in order to fulfil their job role
- sign out and sign in all files removed from the office, so that they can always be located
- make sure that information about employees is not accessible to other people, unless they are entitled to it.

You should not:

- print information unless absolutely necessary
- leave personal or confidential information unattended in the office for any length of time – lock it away
- store personal or confidential information where it can be accessed by those not entitled to see it
- leave personal or confidential information in view of people not entitled to see it, for example on a whiteboard or in view of people looking in through office windows.
- not allow individuals to 'tailgate' you as you enter an EDDC building or office, if you don't know their identity.

Remote working

You should:

- Consider confidentiality when holding conversations or using a screen. Be aware of who might be able to overhear your telephone conversations and position your screen where it is not likely

to be overseen – especially when working in a public place.

- Take care with printed information. At home you will not have access to a confidential waste facility and so you need to safely store printed material until you can take it into the office and dispose of it securely
- Store equipment and documents as securely as possible.
- Use strong passwords and use different passwords for different hardware/systems
- Communicate securely – use communication facilities provided by the council whenever possible, rather than personal devices.
- Always lock your workstation if you leave it unattended for any period of time, even at home

You should not:

- Mix corporate data with your personal data. If you have to use your own device, as opposed to hardware provided by the council, ensure that you keep this data separate and do not retain it on a personal device for any longer than is absolutely necessary
- Leave your laptop, documents or other device unattended in a public place or in your vehicle
- Enable inadvertent access to documents/screens which contain personal data – always carry this type of document securely and so that it cannot be inadvertently read

Carry paper files off site

This guidance covers the correct procedure and additional precautions to take when carrying paper files, containing personal and/or confidential and/or business sensitive information, off-site.

You should always;

- Only carry paper files if absolutely necessary. Consider alternative means of accessing the information from your destination.
- Count how many files you have before you set off and check that you have the same number of files prior to leaving all destinations.
- Ensure that you sign in and out any paper files, in accordance with your service's policies for handling paper files.
- Ensure that your service/team/office operates a tracer card or other similar system for signing paper files in and out of the office.
- If you are keeping sensitive papers with you overnight, do not leave them locked in your car; make sure that they are stored securely inside your property.
- If you intend to visit several clients in one go and need to take out all of their files, where possible, only take in the client's file that you are seeing and keep the rest locked in your car, out of sight.
- Ensure your briefcase, file or bag, contains your name, job title, team name and contact telephone number, in case it is lost or stolen.
- If you have lost or had stolen any files containing sensitive information, contact the Police on 101 and notify the Data Protection Officer on 01395 517401.

You should not;

- Do not take out more information than you really need to.

- Never leave sensitive papers unattended, even for a short time. Lock them away or keep them with you.
- Do not carry loose papers. Carry them in a locked briefcase or in a folder or bag that can be securely closed or zipped up.
- Do not walk around in public, with a file that shows a person's name on the front. Place it inside another file, with no identifying information on.
- Do not put your files or bag on the top of your car, while you open the door. Place it next to your feet, to avoid driving off with it on the roof.
- Do not share or leave any paper files with customers or clients without first fully checking that you are sharing the correct information, and that the content is appropriate.

Sharing of information with Cllrs

This guidance covers providing information containing someone's personal data to Councillors. It is in addition to the guidance in the Council's Constitution which governs the provision of information to Councillors more widely.

Councillors have a number of roles that they fulfil. As a Councillor they sit on various committees and may have certain responsibilities to carry out as part of the Council. In addition they are Ward Members and represent their electorate. They may also represent their political party. Beyond this many will have other roles, either as elected representatives of other tiers of local government (parish / town council or the county council) or other external bodies.

You should always;

- Ensure you understand the capacity in which the Councillors is asking for personal information.
- Where the Councillor is acting in their Ward Member capacity on behalf of a constituent provide the information only where the individual has provided their consent

You should not;

- Make personal comments in correspondence with Councillors (such comments constitute 'personal data' and need to be provided to the data subject if requested) – keep what is said to only what is necessary for the purpose of carrying out the task.
- Provide personal information in the absence of a clear link with the role of the Councillor.
- Provide personal information to the Councillor acting as Ward Member on behalf of a constituent where the consent of the individual concerned has not been given / demonstrated.
- Provide anyone's personal information to a Councillor when they are acting as political party representative with the express authorisation of the Data Protection Officer.
- If there are any doubts you should seek advice from the Data Protection Officer or the Information and Complaints Team.

Disposal of confidential or sensitive papers

This guidance covers the correct procedure for disposal of confidential or sensitive papers. All personal, confidential or sensitive business information held in paper form should be destroyed securely when it is no longer needed. This can be achieved in a number of ways:

- Tear the paper in half three times and place in a confidential waste bin / sack.
- Feed the paperwork into a good quality 'cross-cutting' shredder. Do not use a 'single-cut' shredder as this will only cut your confidential papers into vertical strips and can easily be pieced back together. White paper that has been appropriately shredded can be put into standard recycling.

Anonymise personal data

This guidance covers the correct procedure for anonymising personal data. Anonymisation is the practice of editing information that contains personal data, to such an extent that individuals cannot be identified. This guide explains when to anonymise personal data and how to ensure it is undertaken adequately.

Personal data is any information that enables a living person to be identified, either from the data in question or from that data and other information that might be available to the person receiving the data. This could be information that they already hold, or information that is publicly available, for example on the web or in public records.

If anonymisation is carried out properly and adequately, so that it becomes impossible to identify individuals, then the data is no longer personal data and the General Data Protection Regulations 2016 / Data Protection Act 2018 no longer applies to that data. This can enable information to be shared more easily with third parties.

Remember that you may need to edit text besides obvious identifiers such as name and address. For example, the fact that someone has been treated for a particular medical condition, or visited a particular country, may, alongside other data, be enough to identify them.

What you must do when anonymising personal data;

Ensure that it would be impossible for the individual to be identified. Remember that the recipient of the data you have anonymised may have access to other information that would enable them to identify who the information relates to.

Ensure that any editing you have carried out cannot be undone by the recipient of the data. For example, consider converting an anonymised document to PDF before sending.

Double-check your document when you think you have completed anonymising it, to ensure that you have not accidentally missed any text, and that the remaining text does not allow individuals to be identified.

Ask a colleague to peer-check the document you have anonymised, and confirm to you that you have not accidentally missed any text, and that the remaining text does not allow individuals to be identified.

If undertaking a large-scale project, involving the anonymisation of personal data relating to a large number of individuals, or the regular sharing of anonymised data, you must contact the Data Protection Officer, so that an information risk assessment can be carried out.