Email Procedures regarding Data Protection

The Data Protection Glossary to accompany these procedures is found at on the Newman website.

All Newman University staff need to follow these procedures. Students are encouraged to follow these procedures.

Once you send an email, it is out of the control of the sender what happens to it and how any content of that email is used. Emails are also stored on multiple devices, whose security may be limited and out of our control. Therefore it is important to be very careful what type of information you email and how you do it.

Q1. I need to send someone some personal information, what alternatives are there to email?

Before you email personal data think about whether the recipient could directly access it from MyNewman / iTrent / Moodle / S-drive folder another database etc. If they can do so, they must. It may be practical to establish a limited access folder on the S-drive through which to regularly share personal information to a specific group of people, however be careful not to retain duplicate copies of information unnecessarily.

Where the personal information is directly accessible, your email should simply inform them that the information is available via the relevant source* (e.g. contact details from MyNewman / updated document on the S-drive / new marks on Moodle etc.).

Other advantages of people directly accessing the personal data they need are:

- people always have access to the correct version of the information
- only the required people can be given access
- different levels of access can be given and removed when no longer needed
- mail box quota space is not wasted with attachments
- larger files can be stored

*N.B. You can often place hyperlinks in emails to link the recipient directly with the information. E.g. to link to the S-drive: 1) highlight the text in the email that you wish to become a hyperlink. 2) Right click, select hyperlink. 3) Navigate within the pop up window to the relevant document, click OK.

If you can both access the same folder in the S-drive you could create a password protected folder within that folder and put the information in there. Remember to delete the folder when you no longer need it. Put a reminder in your Outlook for this.

Q2. I have considered the information above and there are no practical alternatives to emailing this personal information. What do I need to consider?

You must consider the classification of the content. See the two tables later in this document.

You must also take into account the volume of personal data in the assessment of the classification of any set of information. Information which in itself would be classified as 'restricted' when it relates to just one individual would need to be classified as 'highly restricted' when it covers 30 of more individuals. This is because the potential damage from unauthorised disclosure is very much higher and therefore the level of control needs to be more highly restricted.

Definitions of the Classifications and How to Email this content

Information Classification	How to email this type of information
Ordinary information is information which is unlikely to identify an individual, is in the public domain or would be unlikely to have a negative impact on the rights and interests of individuals or the interests of the university.	Ordinary information can be in the body of an email containing the data subject's name. No particular controls, other than common sense, apply to 'ordinary information'. However 'ordinary information' should be treated as restricted or highly restricted when combined with information from either of those categories.
Restricted information is information which if disclosed to unauthorised recipients could have a negative impact on the rights and interests of individuals or the interests of the University and would likely be a data breach under data protection laws or a breach of commercial confidentiality. N.B. 'Restricted information' must be classified as 'highly restricted' when it covers 30 or more individuals and is being emailed or transferred by an external hard-drive / USB etc.	When emailing restricted information, do not put the data subject's name in the email subject line. It is up to your professional judgement of the context of the personal data in the email whether you should use the methods described for 'highly restricted information'. Please refer to the footnotes of the Information Classification Table and then ask your line manager if you are unsure.
'**Highly restricted information**' is information which if disclosed to unauthorised recipients would be likely to result in serious damage to the rights and interests of individuals or of the interests of the University would very likely be a data breach under data protection laws or a breach of commercial confidentiality.	For highly restricted information: **1.** If the recipient can access this directly from MyNewman / iTrent / Moodle / S-drive folder etc. they must. **2.** If the content is personal data do not use the data subject's name in subject line. **3.** If the content is personal data you have two options: - If you choose to use the data subject's name in the email, this content must be in a password protected attachment (with the password sent in a separate email). - If you choose to only use the data subject's

Information Classification	How to email this type of information
	student ID / staff iTrent number, this information could be included in the body of an email. **4.** Where the content relates to non-personal data (e.g. it is commercially sensitive) the information must be attached as a password protected document.

Please be aware that the contents of the Information Classification Table below are only general examples of personal and non-personal data. As highlighted in the footnotes and the rest of this document, the amount of information and the combination of information can change the classifications. You are welcome to contact dpo@newman.ac.uk with any more examples to be included in the Information Classification Table.

N.B. 'Restricted information' must be classified as 'highly restricted' when it covers 30 or more individuals and is being emailed or transferred by an external hard-drive / USB etc.

Information Classification Table

Ordinary Information (non-exhaustive examples)	**Restricted Information** (non-exhaustive examples)	**Highly Restricted Information** (non-exhaustive examples)
[1]Anonymised data	[2]Name, Home address and / or phone number	Financial Information regarding individuals e.g. payment information (credit card details), bank account details, information about debts and student fees
Data agreed by data subjects to be put into the public domain.	List of student names alongside their student ID number / or list of staff names alongside their iTrent numbers	[3]Information identified in Equality Act 2010 as 'protected characteristics' i.e. age, disability, gender reassignment, marriage, civil partnership, pregnancy, maternity, race, religion or belief, sex, sexual orientation
Simple list of names	[2]Names and addresses of student	Information on individuals which is classed

[1] For these purposes anonymised data is information which does not relate to a living individual and cannot identify an individual, or does relate to a living individual but cannot identify an individual through other information which is in the possession of, or is likely to come into the possession of the organisation or person processing the personal data.

[2] If the person who needs these contact details can access them from MyNewman / iTrent etc. they should do so. If they cannot access them, consider whether they need to receive them at all.

[3] Sometimes at Newman emails are sent around sharing the news of an individual's life step such as birthday, marriage, civil partnership or birth of a child / adoption. Under data protection laws these emails are personal data processing 'carried out by individuals purely for personal/household activities' and therefore do not count as 'restricted' or 'highly restricted'. If you do not want an email of this kind sent about you, you should inform your line manager.

Ordinary Information **(non-exhaustive examples)**	**Restricted Information** **(non-exhaustive examples)**	**Highly Restricted Information** **(non-exhaustive examples)**
with no other personal data and not in a context which would be 'restricted' or 'highly restricted'.	applicants.	under data protection laws as 'special category data' i.e. race; ethnic origin; politics; religion; trade union membership; genetics; biometrics (where used for ID purposes); health; sex life; sexual orientation or criminal convictions.
Ordinary	**Restricted**	**Highly Restricted**
Corporate contact details where the personal information **is** publically available or does not identify an individual.	Corporate contact details where the personal information is **not** available publically and identifies an individual.	Individual's name **plus** D.o.B **and** passport details, home address and telephone number
Information on individuals available through social network sites where information is provided on condition that it will be in public domain.	Name **plus** D.o.B or national insurance number	[4]Individual's name **plus** national insurance number **and** passport details, home address and telephone number
Final degree classification	Attendance / participation details relating to an existing student.	Scan of identification documentation
Dates of birth (without name)	Student transcript	Academic progression information
Information contained in an organisation's annual corporate report.	Exam / assessment scripts, assessment marks.	Misconduct or Disciplinary information
Information obtained from publicly available directories /regulatory bodies e.g. Companies House / HEFCE.	Examiner's comments on a student's performance.	Preliminary degree classification/ transcript information pending formal approval and any publication.
Information on an organisation's external websites	References for students or staff not containing any 'highly restricted information'.	[5]Future marketing or student fees information not yet agreed to be made public.

[4] Combinations of personal data increase the risk of misuse of data / damage to the individual if received by the wrong person. E.g. a combination of personal details can increase the ability to carry out identify theft.

[5] This is not personal data but is highly restricted and should be in a password protected attachment

Ordinary Information (non-exhaustive examples)	**Restricted Information** (non-exhaustive examples)	**Highly Restricted Information** (non-exhaustive examples)
	UCAS forms not containing any 'highly restricted information'.	References for students or staff containing 'highly restricted information'
	[6]Assessment material prior to "unseen" assessment	UCAS forms containing 'highly restricted information'
	Research grant applications/proposal.	[6]Information relating to restricted intellectual property rights or covered by a confidentiality agreement/ contract.
Ordinary	**Restricted**	**Highly Restricted**
	School children's personal information e.g. full name and information about their academic performance.	School children's personal information e.g. full name and information about any special category data e.g. health, disability, ethnicity, religion…
	CVs (**not** containing D.o.B or personal postal address)	[4]CVs (containing D.o.B or a personal postal address)
	Information relating to supply / procurement of goods/services prior to approved publication.	[6]Information that may be regarded as a trade secret or otherwise highly commercially sensitive.
		[6]Legal advice and other information relating to legal action against or by the University.
		Signed University business contracts
		Unsigned University business contracts if they contain commercially sensitive information.

Q3. How do I manage passwords?

- Do not pick a password which is easy to guess.
- Never use the student or staff's name or number as a password.
- Do not use any password you use to log into your work / home computer.
- You could use a password generator to make sure your password is safe.
- Do not use the same password for everything you send.
- If you regularly send 'highly restricted information' to the same person you could use the same password. In that case pre-agree the password with the recipient and do not send the password each time. If the password is shared outside of this pairing, a new password must be used from then on.
- If as a work team you regularly send 'highly restricted information' to each other and there is no practical way to use the S-drive or database for this information sharing, you may pre-agree a group password. Then do not send the password each time. This password must not

[6] The Outlook global address list includes both student and staff data. Consider the risk of the assessment material accidentally being sent to a student, whether or not they are to sit that particular assessment, as it could be passed on.

be shared outside of the group. If the password is shared outside of the group, a new password must be used from then on.

- Pairing or group passwords should be changed at least every 6 months.
- You should only keep a list of passwords if absolutely necessary. With the 7-zip method below you will only need the password once to password protect or open the file (see step 3 and 4) so the password will not need to be stored. If you are using a pre-agree password system and need to keep a list, this list must be somewhere that only you have access e.g. the Z-drive.

Q4. The email I need to send contains 'highly restricted information'. How do I I create a password protected document?

The purpose of password protecting the attachment is to give it an additional layer of security during email transit. The sender and recipient should be storing the document in a limited access area (such as the appropriate S-drive folder or on their Z-drive, which can only be accessed by them).

a) We recommend you use 7-zip to password-protect a file you are going to email. This programme can password protect many file types including: Access, Excel, PDFs, Powerpoint, Publisher and Word. You can download A Guide for Encrypting and Decrypting with 7 Zip from the Newman website.
b) Transmit the password, using your professional judgement as to whether, in that scenario, it is more secure to do so by phone, in person or by email. Each method carries factors of risk and practicality, therefore you need to make a good decision on a case by case basis.
c) You could consider phoning the password through to the recipient (but do not leave it in a voicemail message) or even tell them in person. However you need to ensure that the password is not overheard or the recipient does not write it down in a place where someone else could read it and use it. If it is not practical to phone them or see them face-to-face you should email the password in a separate email.
d) 7-zip will have left your original file untouched to allow you normal access to it. You can now delete the password protected copy (with the white rectangle symbol).
e) When the recipient 'extracts' the file (by inputting the password) 7-zip creates a copy of the file, which does not need a password to open. The recipient can then delete the password protected version of the file as long as they are storing the unprotected version in a safe folder (i.e. with limited access).
f) When either the sender or recipient no longer need the file or the email, they should delete them.

Q5. The 7-zip method did not work on my operating system / device. What else can I use to password protect a document?

The guides below instruct you how to password protect Access, Excel, Word and Powerpoint documents. You cannot password protect a Publisher document in the same way but these guides show you how to save it as a password protected PDF. This method also applies to PDFs you create in the other Microsoft software listed above.

A Panopto Presentation about password protecting in Microsoft Office

A Helpguide to password protecting in Microsoft Office

Apart from 7-zip the University does not have the technical capacity to password protect documents which are already PDFs, i.e. scanned documents or those received from other sources. If you handle a high volume of scanned documents / already created PDFs and 7-zip does not work on your device please contact dpo@newman.ac.uk who will monitor the risk. Currently for these documents you will need to send an unprotected attachment but follow all the guidance in this document for double checking the recipient and the content of the email.

Q6. I have tried the above two methods. My own device does not allow me to password protect documents. What should I do?

Many devices and operating systems are covered by the two methods described above. If according to the information classification table the document you need to send should be password protected, you will need to use a device which caters for this. That could mean waiting until you are on campus to use a university provided computer.

Q7. What is the purpose of password protecting the attachment, especially if I then email the password?

a) If the email with the password protected attachment is hacked or accidentally sent or forwarded to the wrong recipient, the recipient cannot access the sensitive information. Just because one email is hacked does not automatically mean that the email with the password in it will also be hacked.
b) If you send the email to the wrong person, the recipient cannot access the sensitive information unless you have also sent the same person the password. You are less likely to make the same mistake twice.

Q8. For all emails, what checks do I need to do before I press 'Send'?

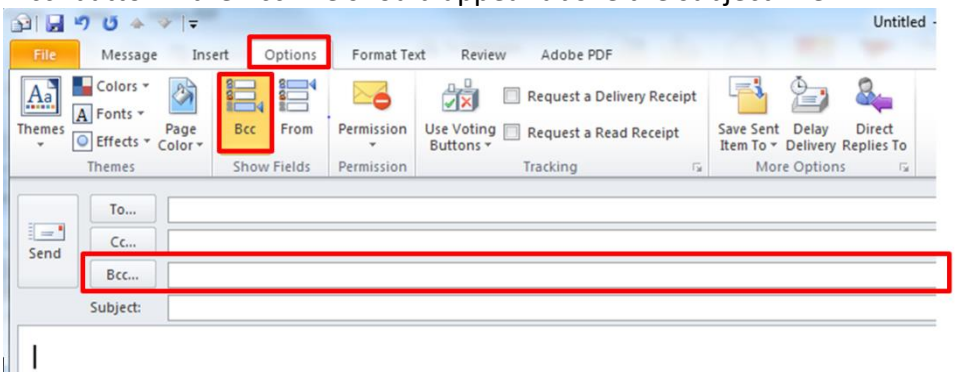
a) Double check all the recipients in the To, Cc and Bcc bars – do they all **need** it? Are the email addresses accurate? Ensure no names have been misidentified, especially as this could mean an email is sent to a student or external person instead of an internal member of staff.
b) When using the global address book, check the Title. All students will have student next to their name, staff should have their job title and
c) Double check the content of all emails within the trail – remove any unnecessary emails below, especially those containing unnecessary personal data including email addresses. If there is any content that one of the recipients should not see, either remove the content or remove the recipient. To remove the content do not simply 'mask' it by changing the font colour or add matching colour highlighting as this can be reversed by the recipient.
d) Double check whether there should / should not be attachments and whether they are / should be password protected.

Q9. The email I need to send is about a sensitive topic but does not contain any personal data. What do I need to consider? E.g. information about a mental health support group:

a) Consider the content of the email combined with its intended audience. Does the combination help to identify something about those people? **A data security breach at another institution occurred when a member of staff emailed generic mental health information to people who had accessed Student Support's mental health services**. The email was accidentally sent to all subscribers in the 'To' bar meaning all the recipients could see each other's email addresses, some of which easily identified the people. **This email should have been sent to all recipients as a 'Bcc' i.e. blind carbon-copy so that everyone's email addresses were hidden.**

b) Double check all the recipients are in the correct To, Cc and Bcc bars. Ensure no names have been misidentified, especially as this could mean an email is sent to a student or external person instead of an internal member of staff.

If you cannot see the Bcc line, in the Outlook email message: from the 'Options' tab, click the 'Bcc' button – the Bcc line should appear above the subject line.



Q10. I have sent an email containing 'restricted information' or 'highly restricted information' to the wrong person, what should I do?

1) Even if the information is pseudonymised or password protected, you need to immediately phone the recipient requesting them to permanently delete the email including any attachments and to respond to you confirming they have done so. If it is not possible to contact them by phone, you need to email them requesting them to do both of these things. Phoning is preferable as it may speed up the response and mean they are less likely to open the email at all.
2) If the recipient has received a password protected attachment but not the password, them deleting the email is the end of the situation.
3) If the recipient has access to the 'restricted information' or 'highly restricted information' (either because the password was also sent to them or because the information was only pseudonymised or not protected at all) you need to immediately report this to the Data Protection Officer as a data breach, preferably for speed by phone (0121 387 4567 or Teams

4567) or if there is no answer then email dpo@newman.ac.uk . This is case whether the email was sent internally or externally.

When making a report, DO NOT INCLUDE 'restricted information' or 'highly restricted information' relating to the breach. Check for attachments and remove them. If you do include the breached data you are causing another data breach.

You need to include:

- The date and time of the data breach (i.e. when you sent the email)
- how the data breach occurred
- what 'restricted information' or 'highly restricted information' is involved
- the number of data subjects affected
- the number of data records affected (e.g. a breach involving the name, date of birth and address of 5 people would be 15 data records)
- who has been given access to the information who should not have access
- whether you know that the information has been accessed
- what remedial action you have taken
- any other information you think is relevant.

The DPO or DPO's representative will respond to you and support you in managing the data breach. Depending on the severity of the personal data breach, the DPO may need to notify the Information Commissioner's Office, for which there is a 72 hour deadline from the time the first person in the organisation knows of the personal data breach. Therefore if you have reported a personal data breach it is vital that you check your email for a response from the DPO, even if this means checking over the weekend.

Q11. What other policies and procedures are there that relate to data protection?

Audio Recording Advice for Minute Taking
Bring Your Own Device (BYOD) Policy
Computing and Networking Facilities: General Conditions of Use
Confidential Waste Procedure
Data Breach Reporting Procedure
Data Protection Getting Sign Ups to a Mailing List and Maintaining it Legally
Data Protection Guidance for Collecting Personal Data about Event Attendees
Data Protection Glossary
Data Protection Impact Assessment (DPIA) Screening Questions Checklist and DPIA Template
Data Protection Lawful Basis Explanations
Data Protection Policy
Data Protection Posters – practical actions
Data Protection Suppression List (Right to be forgotten)
Email Merge from Excel Instructions

Email Procedures regarding Data Protection
Guidance for Handling Personal Data Off-Site
Guidance for Management of Research Data
How to encrypt a memory stick using Bitlocker
Information Classification Table
Information Security Policy
Legitimate Interests Assessment (LIA) Template
New Project Development Procedure – Data Protection
Password Protecting Attachments using 7-Zip – first recommended method as you **do not** need to remember the password long-term
Password Protecting Documents in Microsoft Office – second recommended method, as you **do** need to remember the password long-term
Privacy Notice Template – How to use it
Privacy Notice List and Links
Procedure for Responding to a Data Subject Access Request
Reviewing Contracts – Data Protection Clauses
Virus Management Policy
Wireless Networking Policy