BPP Email Policy in relation to Personal Data, Sensitive Personal Data and Potentially Harmful Data

The General Data Protection Regulation (GDPR) comes into force on 25th May 2018. The GDPR imposes stricter rules in terms of how BPP may collect, use and store personal data in the course of its business. These rules will affect the way we use email in our day-to-day working lives.

BPP recognises that the use of email is an important part of our working practices and therefore this Policy has been created to ensure BPP staff can continue to use emails effectively whilst ensuring BPP's compliance with the GDPR.

Definitions

The following definitions apply to this Policy:

Personal Data: means any information which on its own or when combined with other information available to BPP, can identify an individual. This will include (but is not limited to) data such as names, email addresses, SRN, employee number, photographs and personal addresses.

Potentially Harmful Data: means any Personal Data which could, if disclosed inappropriately, put an individual at risk of identity theft or fraud. This will include (but is not limited to) data such as log in credentials (for email accounts, system accounts, VLE etc.), debit/credit card details, copies of passports or visas (which may also constitute Sensitive Data) and copies of other documents used for proving identity such as bank/council tax statements or utility bills.

Sensitive Data: means any Personal Data relating to health or medical information (including learning support needs or disabilities), criminal convictions (including copies of DBS checks), ethnic or racial origin, sexual orientation, religious beliefs, political opinions and trade union membership.

The following provides guidance for appropriate use of email:

1. Sending bulk or mass communications

When sending out an email to multiple recipients, for example a communication to all students on a particular course or as part of a marketing campaign, you must always use the "Bcc" field and not the "To" or "Cc" field.

a. Under GDPR, the email address of an individual is considered to be personal data even if it is a professional email address. Disclosing other recipients' email addresses, when you have no legitimate basis for doing so, is considered a data breach and must be reported to dataprotection@bpp.com

b. Where possible, consider using software (e.g. mail merge) that allows you to send each email out individually, and always double check emails before sending.

2. Disclosing Personal Data by email

Before sending any personal data by email, please consider if an email is actually necessary, e.g. if you are sending a document to somebody else within your team, could you simply send them a link to the folder where the document is stored on the Shared Drive.

It will sometimes be necessary to share Personal Data relating to students and/or employees by email in the course of business.   Whenever Personal Data is to be shared via email you must follow the following rules:

a. Do not disclose Sensitive Data or Potentially Harmful Data in the body of an email

As emails are not a secure method of communication (and can easily be forwarded/shared without restriction) we should not be disclosing Sensitive Data or Potentially Harmful Data in the body of an email.

We should also not ask or encourage individuals to share Sensitive Data or Potentially Harmful Data in the body of an email (e.g. we should never ask students to send credit/debit card details in the body of an email).

Where Sensitive Data or Potentially Harmful Data needs to be shared by email you must follow the rules on using attachments at paragraph c. below.

Should Sensitive Data or Potentially Harmful Data be accessed by an unauthorised individual this would constitute a serious data breach which must be reported to dataprotection@bpp.com.

b. Do not disclose bulk Personal Data in the body of an email

In the course of business it may be necessary to share Personal Data in the body of an email, for example informing a member of staff that they need to return a call to a student and providing the student's name and contact details.

Where the Personal Data being shared does not amount to Sensitive Data or Potentially Harmful Data it is acceptable to include this in the body of an email.

However, if you are sharing Personal Data about multiple individuals by email (for example reporting to a sponsoring employer on a group of students) this information should not be disclosed in the body of an email and you must follow the rules on using attachments at paragraph c. below.

Should bulk Personal Data be accessed by an unauthorised individual this would constitute a data breach which must be reported to dataprotection@bpp.com.

c. Using email attachments

You must always use **a password protected attachment**[1] (e.g. pdf document, Excel spreadsheet, Word document) when:

- sharing Sensitive Data;
- sharing Potentially Harmful Data;
- sharing large amounts of Personal Data externally, e.g. to professional bodies, employer sponsors, clients etc.;

[1] Instructions how to password protect documents are available in the Appendix.

- sharing large amounts of Personal Data internally, e.g. sending student reports to other BPP employees;
- sending students their exam results; and
- sending any documents to students which could cause embarrassment if sent to the wrong individual (for example applications for mitigating circumstances, documents relating to allegations of academic misconduct etc.).
- **Please ensure that the password is not included in the same email.**

Password protecting documents for students

When password protecting documents for students, each team should make a uniform decision regarding what formula to use when creating passwords.

Suggestions:

- DOB + surname = DDMMYYSURNAME
- SRN (be aware of using this in case you are responding to an email trail where this information is available)

Ensure students are informed of the format of the password (but not the password itself) or sent a separate email with the password. Please also take care to ensure that the password cannot be deciphered from the email trail. This will ensure that only the intended student is able to open the document.

Password protecting documents for clients/external organisations/internal emails

When password protecting documents for clients/external organisations/colleagues, you may select the password, but ensure the password is sent in a separate email to the document or a format agreed with the recipient. Please also ensure that the same password is not used across different clients/external organisations.

Please be aware that the above rules only apply to email sharing. They do not apply to documents shared via Office 365.

3. Consider whether your email contains marketing information

Should you be sending any emails to students or other external parties that contain any information that could construed as marketing[2], it should be sent either centrally by the marketing department or in compliance with BPP's marketing policy.

Any emails that contain marketing information are strictly regulated by both GDPR and the Privacy and Electronic Communication Rules (PECR). It is essential that we abide by these rules.

If you are unsure of whether an email contains marketing information please contact dataprotection@bpp.com for advice. Please be aware that emails advertising BPP or third party courses, programmes, events, seminars or products are likely to constitute marketing.

[2] The action of promoting and/or selling products or services, including conducting market research and advertising. This covers both material relating to BPP products and services and third party products or services.

4. Consider your recipients

Under the GDPR, BPP is under strict requirements not to share any form of Personal Data any more widely than is necessary. Therefore, we should not be disclosing Personal Data to those who do not need it to fulfill their job roles. When sending emails please consider the following:

a. If someone has referred a student query to you, do not automatically copy them back into the full email response to the student to demonstrate you have taken action (i.e. as an FYI). You can notify them separately.

b. When sending an email containing Personal Data, consider who actually needs access to that Personal Data. Do not copy people into emails as an FYI or to show that a particular action has been completed. This can be done in a separate email not containing the Personal Data.

c. When responding to an email containing Personal Data, please consider if all the original recipients need to be copied into the response. Ensure that you remove any unnecessary recipients (including external parties).

d. If you receive an email containing Personal Data that you do not need as part of your job role, delete the email.

5. Use email as a data transfer tool, not a data storage facility

Email is not an appropriate storage facility for Personal Data and will cause issues with GDPR compliance. Accordingly:

a. Sensitive Data and Potentially Harmful Data must not be filed in emails but saved on a restricted access database/restricted access shared drive. Once saved, the email or relevant attachment should be deleted from your inbox/sent items. If you require the email trail for your records, you may either save the email itself into a restricted access folder or acknowledge the contents in your response, e.g. 'Thank you for sending through a copy of your passport, I have now made a note of this on our database'

b. Similarly, important attachments e.g. contracts should be saved in a restricted access database/restricted access shared drive.

c. BPP is introducing a rule where any email older than 6 years[3] will automatically be deleted. This rule will take effect as of 13 April 2018.

6. Active BPP University students should only be emailed to their BPP email addresses

Wherever possible, we should only be using students' BPP email addresses to communicate with BPP University students. This ensures that we have a better control over Personal Data should it be accidentally sent to the wrong student. It also reduces the risk that any marketing material sent to students will breach marketing regulations.

[3] Contractual limit on litigation

7. Use of work or personal mobile to access emails

In addition to the rules set out in BPP's Bring Your Own Device Policy, the following rules are also applicable to the use of work mobile phones and personal mobiles for work purposes:

a. You should only be using your personal mobile phone to login to your emails via email.bpp.com, you should not have emails automatically synced to your personal mobile phone.
b. It is your responsibility to ensure that your work and personal phone are protected by a PIN.
c. Where you are using your work or personal phone to access emails you must not download or save attachments containing Personal Data to your phone.
d. Should you accidentally lose your work mobile or personal mobile which you use for work purposes or have it stolen, you will need to report this to dataprotection@bpp.com as it will constitute a potential data breach.

8. Use of personal laptops / iPads or other computer equipment to access emails

In addition to the rules set out in BPP's Bring Your Own Device Policy, the following rules are also applicable to the use of **personal computer equipment** for work purposes:

a. You should only be using your device to login to your emails via email.bpp.com, you should not have emails automatically synced to your personal device.
b. It is your responsibility to ensure that your device is protected by a PIN or a password.
c. Where you are using your personal device, you must not save attachments containing Personal Data to your device. These must be saved on the appropriate system or shared folder on the BPP network.
d. Should you accidentally lose your device or have it stolen, you will need to report this to dataprotection@bpp.com as it will constitute a potential data breach.

9. Sending Outlook invites to a group of external recipients – how to send as 'bcc'

When sending a meeting invite to a group of external recipients, you should send it as 'bcc' so that you do not needlessly disclose email addresses to other recipients. This can be done by following the steps below:

a. Open a new meeting invite
b. Click on 'to' field button
c. Enter email addresses in the 'resources' field either by selecting from the address book or by copying and pasting
d. Click OK
e. Delete the email addresses from the **location** field and enter correct location details
f. Click send

Please be aware that any email addresses added directly in the 'to' field will be visible, they must always be added as a resource and then deleted from the location.

Please be aware that any breach of this policy will be treated as a disciplinary matter. If you have any questions or are unclear about any of your obligations under this policy please contact dataprotection@bpp.com.

APPENDIX

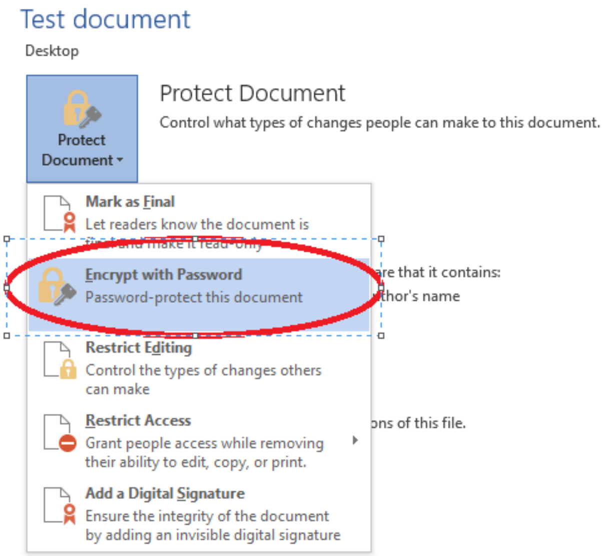
Password protecting a pdf

Follow the steps below to add a password to a pdf:

1. Launch Adobe Acrobat Pro
2. **File** > **Open**
3. Select the PDF to open
4. Click or tap on **'Open'** button
5. **File** > **Properties**
6. **Properties > Security tab**
7. **Security Method** > **Password Security**
8. Check **"Require a password to open the document"**
9. Enter a password to protect the PDF.
10. Save the PDF and quit Adobe Acrobat – **ensure that you 'save' otherwise the password isn't!**
11. Once saved when the pdf is open it has (SECURED) after the name at top left of screen

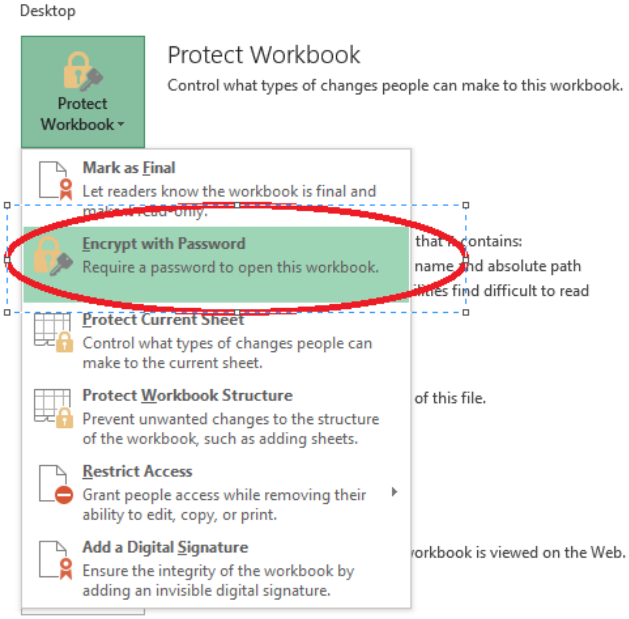
Password protecting a word document

Go to File>Protect document>Encrypt with password


Test document
Desktop
Protect Document
Protect Document
Control what types of changes people can make to this document.
Mark as Final
Let readers know the document is final and make it read-only
Encrypt with Password
Password-protect this document
re that it contains:
thor's name
Restrict Editing
Control the types of changes others can make
Restrict Access
Grant people access while removing their ability to edit, copy, or print.
ons of this file.
Add a Digital Signature
Ensure the integrity of the document by adding an invisible digital signature

Password protecting an excel spreadsheet

Go to file>Protect workbook>Encrypt with password



Protect Workbook

Control what types of changes people can make to this workbook.

Mark as Final
Let readers know the workbook is final and make it read-only.

Encrypt with Password
Require a password to open this workbook.

Protect Current Sheet
Control what types of changes people can make to the current sheet.

Protect Workbook Structure
Prevent unwanted changes to the structure of the workbook, such as adding sheets.

Restrict Access
Grant people access while removing their ability to edit, copy, or print.

Add a Digital Signature
Ensure the integrity of the workbook by adding an invisible digital signature.