Data Privacy

THE DO'S AND DON'TS BOOKLET ON DATA PRIVACY

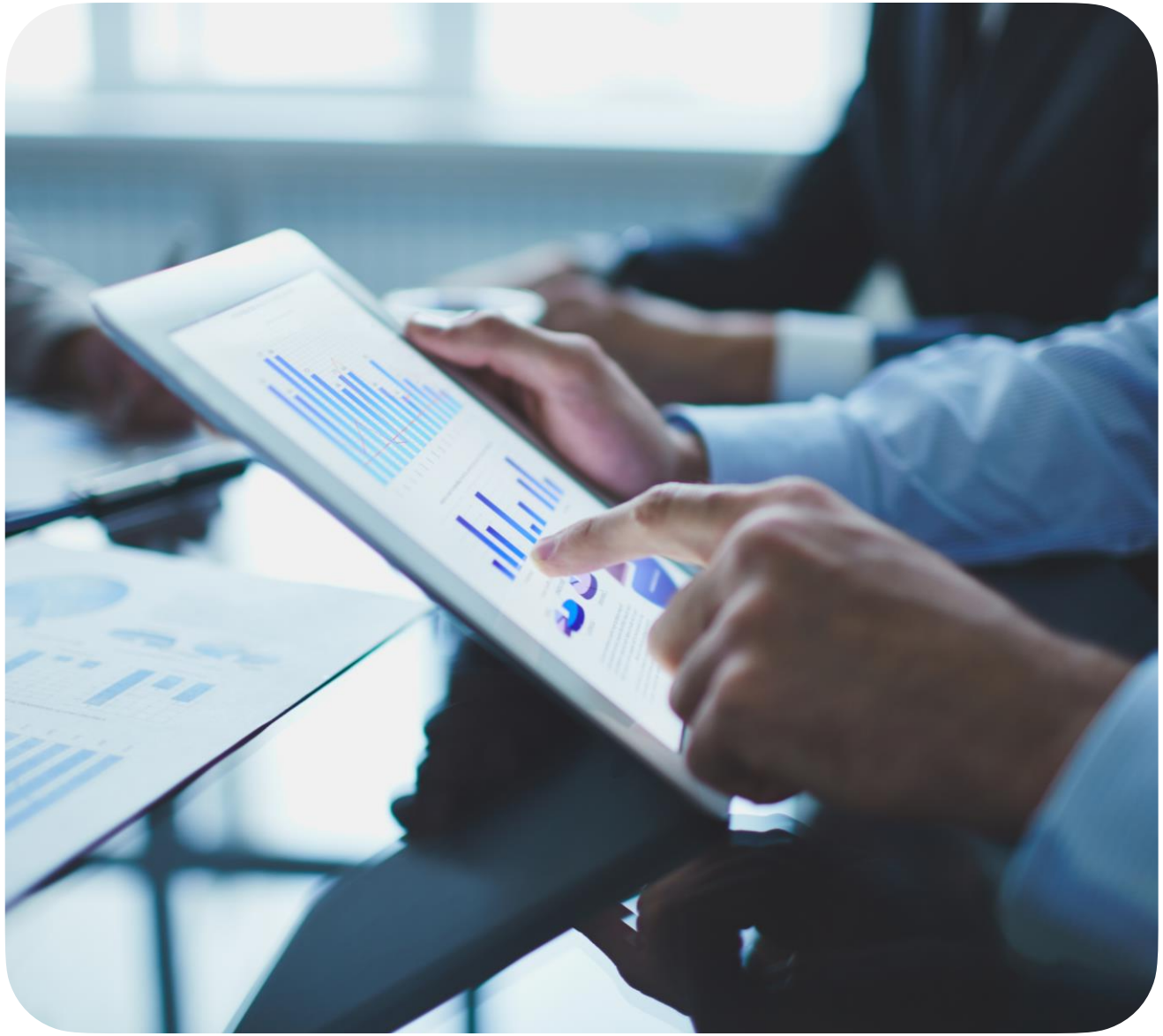
MCM XXIII

1923 INVESTMENTS

HARVEST

+ Within the booklet are a few simple practices we must all adopt to have effective data privacy measures.

+ Please take some time to read through and familiarise yourself. This booklet should be kept handy for ease of reference.



The **DO'S** - E-mail

DO	WHY?
Check attachments containing personal data before sending by e-mail.	We must ensure that we share the correct data both with external parties as well as with colleagues.
Double-check the recipient(s) before sending out an e-mail. Always check all recipients especially when using the 'Reply all' function and ensure that the recipients are correct and in the correct 'To/Cc/Bcc' section. Be careful of 'auto complete' when selecting addresses as it is very easy to select the wrong person with the same name.	Many data breaches occur due to e-mails being sent to the incorrect recipient.
Password protect spreadsheets containing bulk confidential data being sent internally to colleagues by e-mail.	Password protection ensures that if an e-mail is sent erroneously to an external recipient instead of an internal colleague the external recipient cannot access the data in the document.

The **DO'S** - Mail

DO	WHY?
Double-check the recipient details before sending out any postal mail.	Ensure that envelopes and their content do not get mixed up when sending out physical mail. If possible, also ensure that the address is correct since customers can move residence. .

The **DO'S** - Securing Data

DO	WHY?
Report to your line manager or head of department if a customer is making a request out of the norm that you are unfamiliar with. Do not share data before you confirm the legitimacy of the request.	Unusual requests may pose risks to data security and privacy. Reporting ensures that the organisation can assess the situation and take appropriate action before sharing any data.
Always save important documents on specific secure repositories such a department or function drives or sharepoint sites.	Employee outlook and one-drive accounts will be deleted in line with company policy once employment is terminated leading to the deletion of important documents that could potentially pose a serious business continuity issue to the company.
Put all documents away under lock and key in your desk or cabinets when leaving the office.	Our customers trust us with their information and also the information of their customers and we have to ensure that this data does not get in the wrong hands.
When attending to customers, keep only documents (electronically and physically) pertaining to that client.	To ensure that customers do not view documents pertaining to other customers.
Keep as little as possible on your desk during the day.	Can you honestly list and recall all the documents you have on your desk should they get mislaid? Be organised and in control of your work.
Lock computer/laptop screens every time you leave your desk. Always press Windows key+L to lock your screen.	It is your responsibility to secure access to your computer. Remember that all the transactions or e-mails that pass through your computer or laptop are identified by your user.

The **DO'S** - Data Breaches

DO	WHY?
Immediately advise your line manager or head of department if you notice any suspicious activity or a potential data breach.	Any situation should be resolved immediately - Do not wait to escalate.

The **DO'S** - Remote Working

DO	WHY?
Ideally do not take any physical data out of the office when working remotely or attending external meetings – all data should be kept on secure devices such as company devices.	This reduces the risk of loss of confidential information or commercial information.

The **DO'S** - Document Destruction

DO	WHY?
Ensure that when placing items in the shredder they actually drop down and are completely shredded.	If the shredder gets stuck and documents are not completely shredded they can be retrieved defeating the scope of discarding documents through this secure machine.

The **DO'S** - Passwords

DO	WHY?
Ensure that you have robust passwords.	A strong password acts as a barrier against unauthorised individuals attempting to gain access to your accounts or sensitive information. It also prevents hackers, cybercriminals, and malicious actors from easily guessing or cracking your password.

The **DO'S** - Printing

DO	WHY?
Ensure that you collect any printing containing confidential data immediately and check that you remove all documents being photocopied. Use printing passwords where available.	It is very easy to get distracted at the printer. Don't walk away before printing is finished as someone else may pick it up.
Only print what you need without making unnecessary copies.	Besides the waste of paper that is not aligned to the corporate social responsibility adopted by the organisation, having extra papers only serves to increase the risk that these might fall in the wrong hands.

The **DO'S** - Social Media

DO	WHY?
Be careful what you share on your personal social media sites and never put the organisation at risk by divulging confidential data.	Think before you post – once posted you cannot control who views and shares your post and in seconds could be seen by hundreds if not thousands.

The **DON'TS**

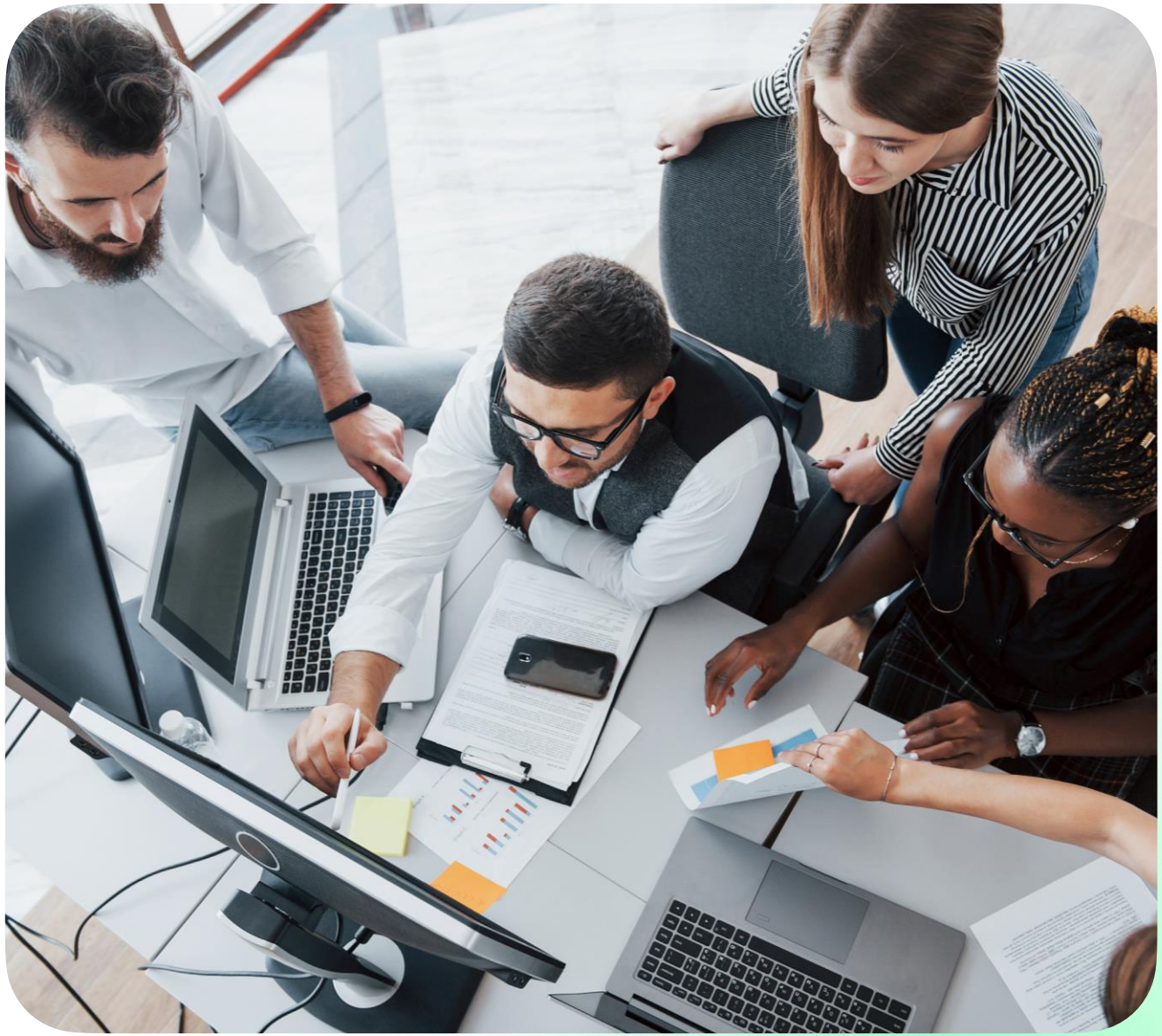
DON'T	WHY?
Click on any links or open attachments, on any e-mails that you receive that you think are not legit. Report on 'Phish Alert report' and follow their instructions.	Phishing involves tricking people into disclosing confidential information through electronic communication such as e-mails. These messages, which are disguised to look legitimate, can also trick recipients into clicking on links or opening attachments that infect IT systems with malicious software and viruses.
Send customer/company confidential information to your personal e-mail account.	This is a serious breach and disciplinary action may be taken.
Leave company devices unattended in public spaces.	These items are small and can be easily stolen. It will be gone before you know it!.
Dispose of any personal data in the normal landfill waste bins.	Shred personal data within the appropriate shredder.
Discuss customer/company confidential information in public spaces.	The company has professional secrecy and confidentiality obligations which must be kept in mind at all times.

Help & Support

Your Data Protection Officer is available to provide you with advice and guidance that will help you keep data Safe and Secure.

If you experienced a data breach of confidentiality, availability or integrity, report it immediately to the Data Protection Officer on the following e-mails no later than ‘close of business’ of that same day:

+ dataprivacy@1923investments.com
+ dataprivacy@harvest.tech
+ dataprivacy@ptl.com.mt
+ dataprivacy@apcopay.com
+ dataprivacy@apco.tech



Thank You

MCM XXIII

1923 INVESTMENTS

HARVEST