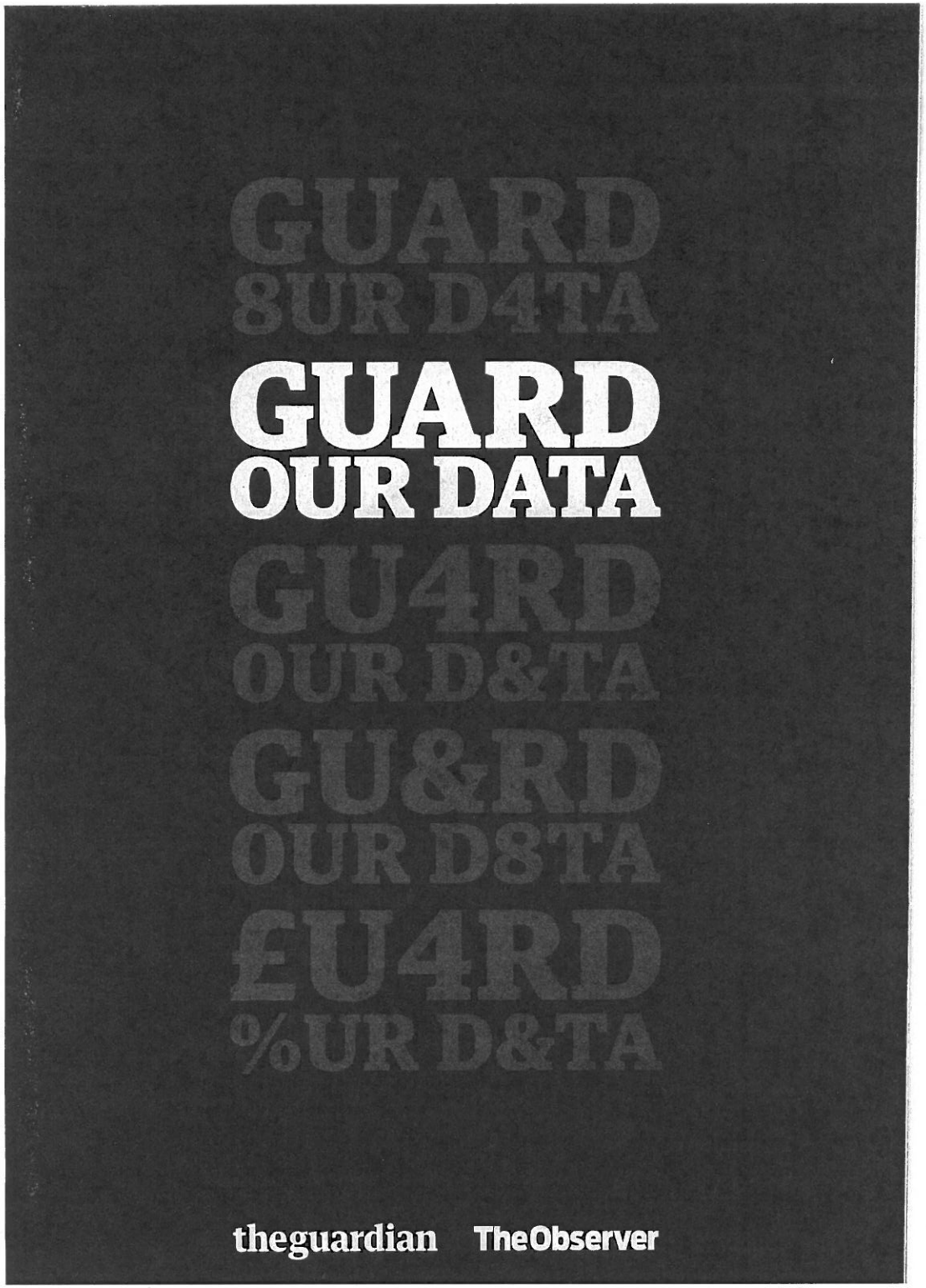

GUARD
8UR D4TA
GUARD
OUR DATA
GU4RD
OUR D&TA
GU&RD
OUR D8TA
£U4RD
%UR D&TA
theguardian
TheObserver

Welcome

Guarding our data helps us maintain customer trust, and helps to prevent the reputational and financial damage that could be caused by the loss or theft of confidential and personal data with which we have been entrusted.

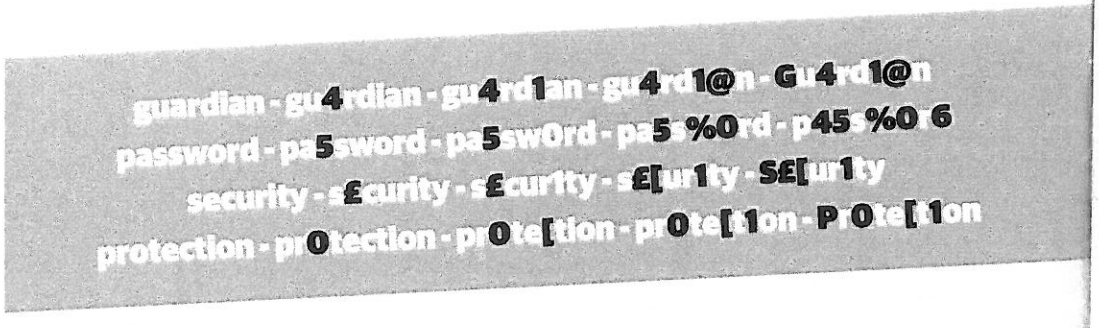
We all play an important role in protecting the data we collect and use. This guide contains some simple actions you can take on a daily basis.

Please could all staff take a short while to read this document, and contact the Information Security and Risk team if you have any questions or need further guidance.

Thank you.

Andrew Miller, CEO

Why do I need a good password?



Strong passwords reduce the likelihood of unauthorised account access.

- A good password is at least 8 characters long and a mixture of numbers, letters and symbols.
- Do not write down your passwords or share them with anyone.
- Change your passwords every few months.
- Do not use the same passwords for work and personal accounts.
- If you suspect your password has been compromised, change it immediately and inform your line manager.
- Computing and mobile devices should be locked with a password when left unattended.

Can I use removable media and portable devices at work?

Removable media

These include USB keys, external hard drives, CDs/DVDs and MP3 players. You might use these to back up data when working outside the office or to transport a presentation to a meeting. Personal GNM data should not be stored on removable media.

If you connect removable media to a non-GNM system, or receive them from a third party, always virus scan them if you then attach them to GNM systems.

The Technology Service Desk (Ext. 34444 or via 34444@guardian.co.uk) can assist you with both encryption and virus scanning.

Portable devices

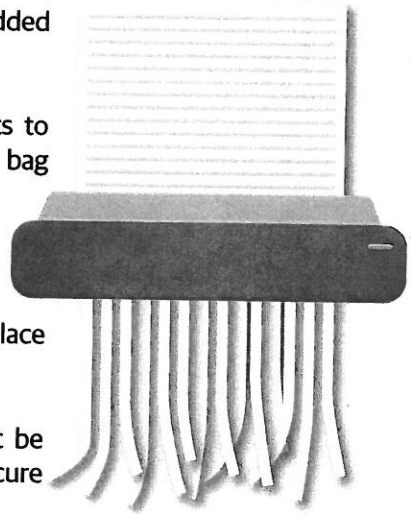
These include smartphones and tablet devices. You may access your work email via an exchange email account (for further information on exchange accounts go to https://sites.google.com/a/guardian.co.uk/frequently-asked-questions/Home/mobile/iphone-and-ipad), or, by using the built-in browser using two-factor authentication.

You should not save documents containing personal GNM data (e.g. customer spreadsheets, staff data) on to a personal device.

How do I dispose of confidential information?

Insecure disposal of confidential and personal information could cause harm to GNM and/or the individuals to whom the data relates.

Such paper documents should be shredded and **not** placed in the recycling bins.



If you have large quantities of documents to dispose of, request a confidential disposal bag from Workplace Management (Ext. 33333 or via workplacehelpdesk@guardian.co.uk)

CDs and DVDs containing confidential or personal data should be given to Workplace Management for secure destruction.

USB keys and fixed storage devices must be handed to Technology Service Desk for secure destruction/wiping.

How do I keep data safe in an open-plan office?

Physical security plays an important role in protecting data.

Staff should carry their security passes with them at all times.

Maintain an awareness of security in GNM buildings and only allow access to individuals who are known to you.

Ensure any confidential hardcopy or electronic information is secured and locked away as appropriate.

Lock your computer screen when left unattended.

Working outside the office

If you need to work from home regularly, you should discuss with your line manager if it is appropriate for you to have a GNM laptop.

If you have a GNM-issued laptop the hard drive should be encrypted. If you have not been contacted about encryption, please contact the Technology Service Desk (Ext. 34444 or via 34444@guardian.co.uk)

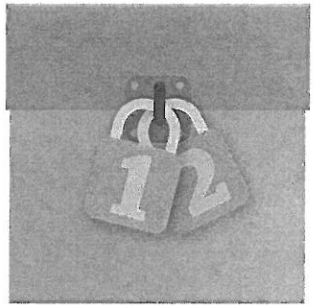
Always remember to shut down your laptop when you have finished working, or if leaving it unattended. Hard-drive encryption only protects computers that are shut down.

Do not leave your laptop where it can be easily seen, e.g. through windows, or when non-GNM staff access your premises – for example, cleaners, removal staff, builders.

You should not save any documents that contain personal or confidential GNM data onto devices that are not owned by GNM.

How do I work safely outside the office?

Use two-factor authentication to log in to your email. Visit Spike and search 'two-factor authentication' for further information.



Do not choose the 'remain logged in' option when logging on.

Always sign out from your account when you have finished.

Do not save documents containing personal or confidential data on to non-GNM devices.

Be mindful of who can see or hear what you are working on.

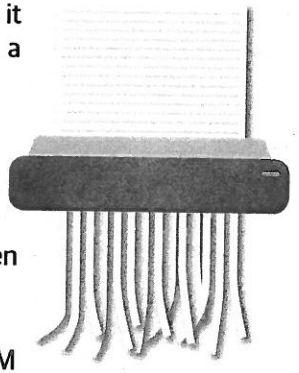
If working from home regularly, make sure you have somewhere safe to store GNM devices and printed documents.

Shut down laptops when you have finished working and do not leave them in sleep/hibernation mode.

If using a personal laptop for remote working, it must have robust anti-virus software.

Security of devices and documents at home

If you have a GNM issued laptop, you should store it somewhere safe when it is not being used, such as a locked cupboard.



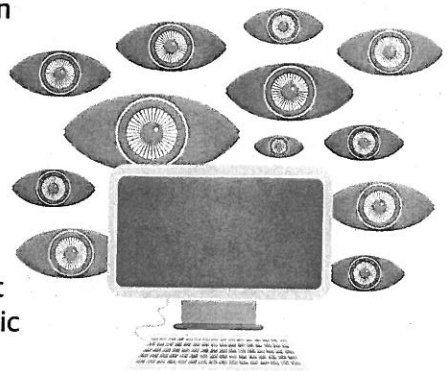
The same rules apply to paper records – only take documents out of the office if absolutely necessary and with your line manager's approval, keep them safe during transport, and store them securely when you have finished working.

Paper records containing confidential or personal GNM data need to be disposed of safely. If you have a cross cut shredder at home, you can use this, otherwise return the documents to the office for disposal.

Working in public and travelling

Be mindful of who can see and hear what you are working on, for example when working on trains or planes.

If you do need to work in public, obtain a privacy screen for your laptop via Workplace Management (Ext. 33333 or via workplacehelpdesk@guardian.co.uk) to make it more difficult for people to see what you are working on.



Do not leave any computing equipment unattended when travelling on public transport.

If you are away overnight, make use of your hotel safe to store your laptop or papers, or obtain a Kensington lock so your laptop can be secured to an immovable object. Do not leave GNM IT equipment in the boot of your car overnight.

If travelling by car, and you have to leave your laptop unattended, do not leave it where it might be seen. If absolutely necessary to leave it unattended, make sure it has been shut down, and stored in the boot of your car.

Travelling internationally

Customs officials may have the right to inspect the contents of your laptop, and even to detain it. If customs do detain your laptop, please let the Information Security & Risk team know.

You should deal with any requests co-operatively, and follow the instructions of the customs officials.

We suggest that prior to travelling, you clear your computer of any documents which you would not wish customs officials to see, or which may be deemed insensitive or illegal in the country to which you are travelling.

Some countries have restrictions on encrypted laptops. If you are travelling internationally with an encrypted laptop, please consult the Information Security and Risk team for advice.

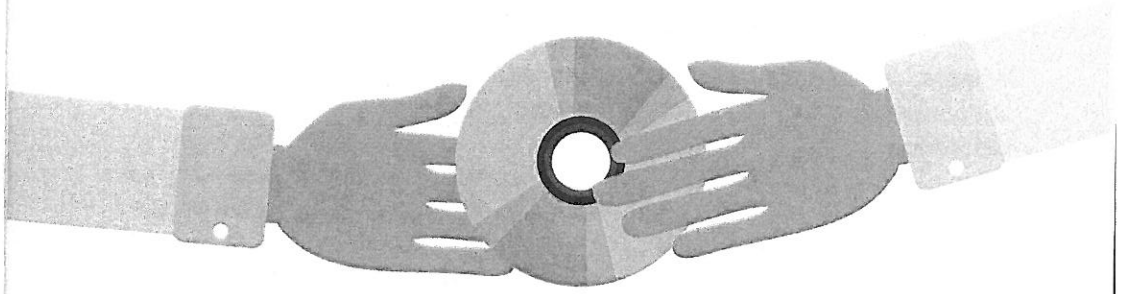
Restriction on travel - The FCO (Foreign and Commonwealth Office) provides a travel restriction advice service, that should be viewed when deciding on travelling to certain parts of the world. The advice covers areas such as safety & security, local laws, any entry requirements, health or natural disasters.

Please follow this link http://www.fco.gov.uk/en/travel-and-living-abroad/travel-advice-by-country/ for up to date travel information.

Can I share data with third parties?

GNM often shares data with third parties for good reason; for example, to aid digital development, to provide expertise, and to help conduct email marketing.

We retain legal liability for personal data that we share with third parties, and it is our responsibility to ensure that the third party is able to protect the data.



Staff must contact the Information Security and Risk team prior to sharing data with third parties to ensure that they have been through the GNM third party review process.

Personal and confidential information must only be transferred to third parties securely. If you are unsure how to do this, contact the Information Security and Risk team.

Sharing GNM data for personal gain is a criminal and disciplinary offence.

Email essentials

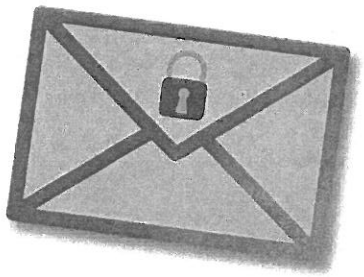
Consider whether the content of your email requires enhanced protection. Attachments containing personal or confidential GNM data (e.g. staff details, contact lists) may need to be password protected.

If you need to transfer personal or confidential GNM data to third parties, please contact Technology Service Desk (Ext. 34444 or via 34444@guardian.co.uk) or the Information Security and Risk team to make sure you are sending it securely.

When you start to type in an email address, Gmail will suggest similar addresses you have used before. Make sure you choose the right address before you click send.

Use blind carbon copy (bcc), not carbon copy (cc) when emailing lists of people who would expect their address to be kept confidential. When you use cc every recipient of the message will be able to see the address it was sent to.

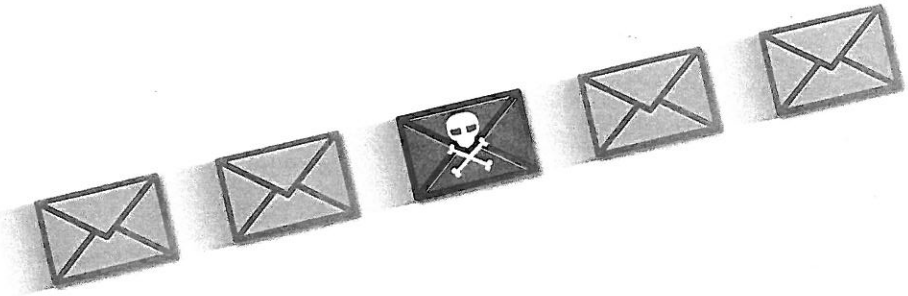
Limit the circulation of email to those who need to see it.



Keep safe

- Do not send any emails containing information about other people that you would not be happy for them to see. The Data Protection Act allows people to request a copy of the personal data we hold on them, and this includes the contents of email (although there are exemptions for personal data used for journalistic purposes).
- Be wary of people who may try to trick you into disclosing personal data.
- Do not trust emails that ask you for account, password, or payment information, as this could be a scam to get you to reveal secret information ('Phishing').
- If you receive spam , do not respond to the email. You can report the email as spam using the 'report spam' option.

Please be reminded that unauthorised disclosure of information may constitute a criminal offence. An example would be sharing company data for personal gain.



Happy faxing

Faxing can easily result in data being sent to the wrong recipients.

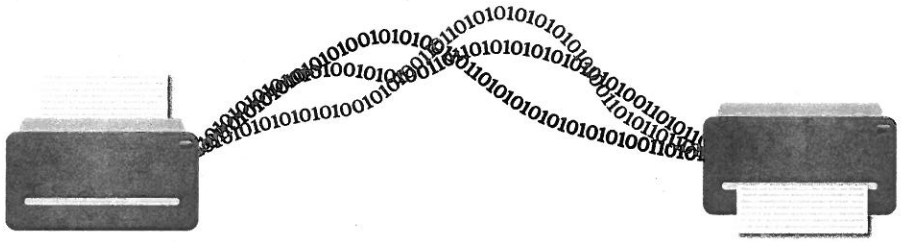
Consider whether sending the information by a means other than fax is more appropriate, such as secure email. Make sure you only send the information that is required.

Double check the fax number you are using.

Check that you are sending a fax to a recipient with adequate security measures in place. For example, if you are sending a sensitive fax it shouldn't be left uncollected in an open plan office.

If the fax is sensitive, ask the recipient to confirm that they are at the fax machine and are ready to receive the document.

Use a cover sheet. This will let anyone know who the information is for and whether it is confidential, without them having to look at the contents, and they will know who to contact if the fax is misdirected.



What do I do if I lose personal data or it is stolen?

Loss or theft of personal or confidential data could put us or our customers at serious risk. All incidents need to be reported to the Information Security and Risk team.

Examples of loss or theft might include:

- sending an email containing personal or confidential data to the wrong recipient.
- losing a file or mobile device that contains personal or confidential data.
- a technical issue which has led to personal or confidential data being breached.

If you lose personal or confidential data or have it stolen you must report it using this form (https://sites.google.com/a/guardian.co.uk/infosec-risk/home/report-data-loss-or-theft).

This will help us to manage the loss of the information and provide further controls or training. We may also have an obligation to report the loss.

If you think the loss or theft is very serious, please contact us immediately - this includes evenings and weekends. Our contact details are on the next page.

How can I get further information and contact you?

For further information please visit the Information Security and Risk site (https://sites.google.com/a/guardian.co.uk/infosec-risk/). This includes our information security and password policies, and a link to the online form to report the loss or theft of personal data.

Contacts

Email:
infosec@guardian.co.uk

Phone:
Dave Boxall (Technical Security Manager)
+44 (0) 20 3353 3089 / 07825 196 330

Tim Gough (Data Protection Manager)
+44 (0) 20 3353 3709 / 07717 807 906

Sarah Walsh (Director of Information Security and Risk)
+44 (0) 20 3353 4053 / 07979 700 539