Information Security
Data Management Plans for your Research

Sara McAneney
Information Security Manager
Date 14/03/18

Why is information Security Important?
Security Protects your Research Data

1. Availability
   Protect against Computer/laptop/mobile device/storage device loss, theft or malfunction

2. Integrity
   Protect against corruption, unauthorised access resulting in Inaccurate, inconsistent, incomplete Data

3. Confidentiality
   Protect against unauthorised access and disclosure of data

Information Security – What do I need to know?

1. General Data Security Day-to-Day good practice
2. Watch out for Scams and Frauds
3. Security in your Data Management Plan
4. Identifying, Classifying and Anonymising data
5. Secure Data Storage and Transfer
6. Technological Tools for Security
7. Considerations for Cloud Computing
General Data Security Day-to-Day good practice

**Update, Update, Update!**

- All software companies are constantly releasing patches and updates to fix security issues, as well as other flaws discovered in their products. You may have heard of the recent Spectre and Meltdown vulnerabilities. These flaws are what virus writers and hackers exploit to gain access to your data.
- Make sure you stay ahead of the hackers and keep your software up-to-date and don’t forget about your tablets and phones.

*Top Tip: Stay current with the latest security updates for your software.*

---

General Data Security Day-to-Day good practice

**Protect against Viruses, Malware and Ransomware**

- If you are using a Windows PC or Apple Mac on the Trinity network in offices and labs then as part of your setup to join the network you will have McAfee anti-virus protection installed and also a service that keeps your Windows computer up-to-date.
- Anti-virus software protects you and your devices from viruses and ransomware which can damage your devices and data.

*Top Tip: Make sure that your anti-virus software is up-to-date and scan your computer regularly for viruses.*
General Data Security Day-to-Day good practice

**Practice good password management.**

- Use a strong mix of characters, don’t share your password with others
- Use different Passwords for all your Internet Services such as Facebook, Twitter, Amazon etc
- If you find it difficult to remember all your passwords, consider using a password manager tool like Password Safe. This tool will save all your passwords securely on your computer.

*Top Tip: Always change your password if you suspect that it has become known to others.*

---

General Data Security Day-to-Day good practice

**Remember to Protect your Mobile Devices**

- Laptops, Smartphones and tablets are all at risk from loss or theft. All laptops storing confidential Trinity Data should be encrypted. This means that data on the device cannot be accessed inappropriately.
- To protect your smartphones and tablets you should have a look at the security features that are available in your device. All devices should have security settings, though the exact options available will differ depending on manufacturer, model and software version.

*Top Tip: Make sure your phone or tablet automatically locks and has a (PIN) set to protect your data if the device is lost or stolen*
General Data Security Day-to-Day good practice

Exercise Caution Online

• Every time you turn on your computer, open an email attachment, click on an unfamiliar link while browsing the Internet you could be putting yourself and your information at risk.

• Don’t store your passwords in your browser. This may seem like a handy feature however this mean that all your passwords are stored in one location on your computer, this might make it easier for someone to obtain them if your computer is compromised.

• Make sure your Browser is up-to-date - Whether you use Chrome, Safari, Firefox or Microsoft Edge, make sure you are running the latest version.

Top Tip: Realise that you are an attractive target to hackers. Don’t ever say “It won’t happen to me.”

Take care when using Public Wireless Networks

• Configure your Wi-Fi settings so that that your computer asks permission to join a new wireless network.

• If you are not using a VPN then do not use public wi-fi to check online banking, purchase items online or access any sensitive Trinity Information.

Top Tip: Always look for secured connections, those that use HTTPS and SSL. Look for the lock symbol in your browser like below:
General Data Security Day-to-Day good practice

Backup all your Data

Backing up your data protects it from loss, theft and corruption. You should backup your data daily or weekly & to multiple locations.

Identify what to backup

- Backup files Documents, images, music, videos etc.

Backup locations

- Hard drive, USB device, External hard drive  Cloud e.g. Google Drive, Dropbox, iCloud

- Top tip: If you are backing up to a physical media such as a harddrive make sure you store it securely e.g. in a fireproof safe etc.

Dispose of Equipment Securely

- When disposing an old device, following the standard electronic waste disposal procedures, if the device contains sensitive or confidential data then you should first remove the relevant storage media e.g. the hard drive, and arrange for it to be securely destroyed, or securely stored for future destruction.

Be aware of scams and fraud

• What kind of scam emails might I find in my inbox?

Phishing Emails
How can I identify a phishing email?

1. It is easy to be alarmed by a phishing email, they are designed to get us to act without question. To avoid these types of scams you need to be vigilant and cautious, always take your time and consider the validity of what you are being offered.

2. Make sure you can confirm the identity of the company or individual with whom you are engaged in a transaction.

3. You can always check the validity of official communications coming from IT Services which are on a secure section of our website, where you will be prompted for your username & password or directly with the IT Service Desk.

4. Never provide sensitive personal information by email or at an unfamiliar website link provided in an email.

What should I do if I receive a phishing email?

- If you have responded to a phishing message, or clicked on any links within the email body and entered your Trinity username and password information, the very first thing you should do is change your password.

- You can do this easily by logging into TCD Password Manager (https://password.tcd.ie).

- The best way to prevent a phishing attack is to make yourself aware of it.

- IT Services will NEVER EVER ask for your username and password via email and you can confirm any communications from us with our website www.tcd.ie/itservices or with the IT Service Desk.

- You can learn more about phishing on the IT Services website (https://www.tcd.ie/itservices/security/phishing.php).
14th March 2018

Security in your Data Management Plan

Identifying and Classifying your Data

1. Identify all data which will be collected, communicated, processed, stored, derived, reported on etc.
2. Classify the Data; Critical, Sensitive, Internal, Public
3. Identify security controls, processes and procedures for each category
4. Identify any External Considerations
Anonymisation and pseudonymisation as a security control

- **Anonymisation and Pseudonymisation** are useful tools for allowing manipulation of data while protecting the privacy of data subjects.

- Data is anonymous if no one, not the researcher, the subject, or any third party can connect the data to the individual who provided it. Anonymisation is irreversible.

- "Pseudonymisation" of data means replacing any identifying characteristics of data with a pseudonym, or, in other words, a value which does not allow the data subject to be directly identified.

- **Note:** Irreversibly and effectively anonymised data is not “personal data” and the data protection principles do not have to be complied with in respect of such data. Pseudonymised data remains personal data.
Can you be sure the Data is Anonymous?

- 2013 MIT Study on mobility - 1.5 million sets of ‘anonymous’ mobile phone location data over 15 months inside a small European country.
- Found that just four points of reference was enough to uniquely identify 95% of participants.
- A few Twitter posts could potentially provide this info

Technical Tools to Protect Data when storing and transferring electronically

- Access Controls – Passwords, biometrics, pins, 2 factor verification etc
- VPN – Virtual Private Network
- Password Management Tools
- Anti-Virus software
- Firewalls
- Log files & Audit trails – very useful in minor breach situation
- Encryption, Disk, File, SSL
Encryption

- Full Disk encryption – A must for data collectors in the field
- File/folder encryption – A must for data transfers e.g. from the field back to HQ - by email, or portable media such as USB drives
- SSL – web traffic encryption - A must for data held in internet accessible portals/storage

Selecting Encryption Software

- Strong Algorithm PGP, AES
- Easy to Use
- Encryption Key Backup/Administrator Override
- Seek professional advice
Don’t...

Procurement of IT & Data Services

• Tender should include Security Criteria
• Smaller procurements should evaluate Security of Service
• Look for evidence of good practice
  • does the company have a security policy, external certification, external auditors
• Strong Contracts and Non-Disclosure Documents, Data Processing Agreements
• Documented procedures
Cloud (Internet) Services

Public vs. Private Cloud
Evaluate the security in place
  – Security Policy
  – External Certification ISO27001
  – External Audit
Contracts – Seek professional advice

Third Party Processors - Agents and sub-contractors

✓ There must be a written contract in place
✓ A data controller must be satisfied that personal data will be secure if it is outsourced to a third party/cloud provider.
✓ Non-compliant Data Processor open to legal action from Data Controllers and Data Subjects and sanctions from the Regulator – i.e. Fines.
Data Processor Compliance

Must keep records of processing, demonstrate appropriate technical and organisational controls

Data subjects may enforce rights directly against Data Processors

Non-compliant Data Processor open to legal action from Data Controllers and Data Subjects and sanctions from the Regulator – i.e. Fines.

Considerations for public “Free” cloud

E.g. Dropbox, Google, SurveyMonkey

1. Read the contract
2. Who owns the data?
3. Under what circumstances can the service be curtailed?
4. Where is the data stored geographically, are there data protection implications?
Further information and Assistance – IT Services
Website http://www.tcd.ie/itservices/security/

Thank You