



Data Protection issues in School Administration

Cyril Drury
JMB Data Protection Advisor

0

Examples of issues related to GDPR

- request for pupil info from public service body (e.g. Dept of Ed/ HSE/ Dept of Social Protection)
- local journalist telephones looking for information about a competition winner
- former student looking for information concerning their time in school
- contractor carrying out work in the school office
- message sent in error to wrong (possibly unknown?) email address

www.jmb.ie

1

1

Data Protection Responsibilities ...within our School

| | |
|--------------------------------|--|
| Board of Management | Data Controller |
| School Management Team | Implementation of Policy |
| All Staff | Adherence to the Data Processing Principles |
| Entire School Community | Awareness and Respect for all Personal Data |



***What are our
responsibilities in
relation to
personal data?***

www.jmb.ie

3

3

Principles... *statutory framework that governs every processing activity...*

- lawfulness, fairness and transparency
- purpose limitation
- data minimisation
- accuracy
- storage limitation
- integrity and confidentiality
- accountability

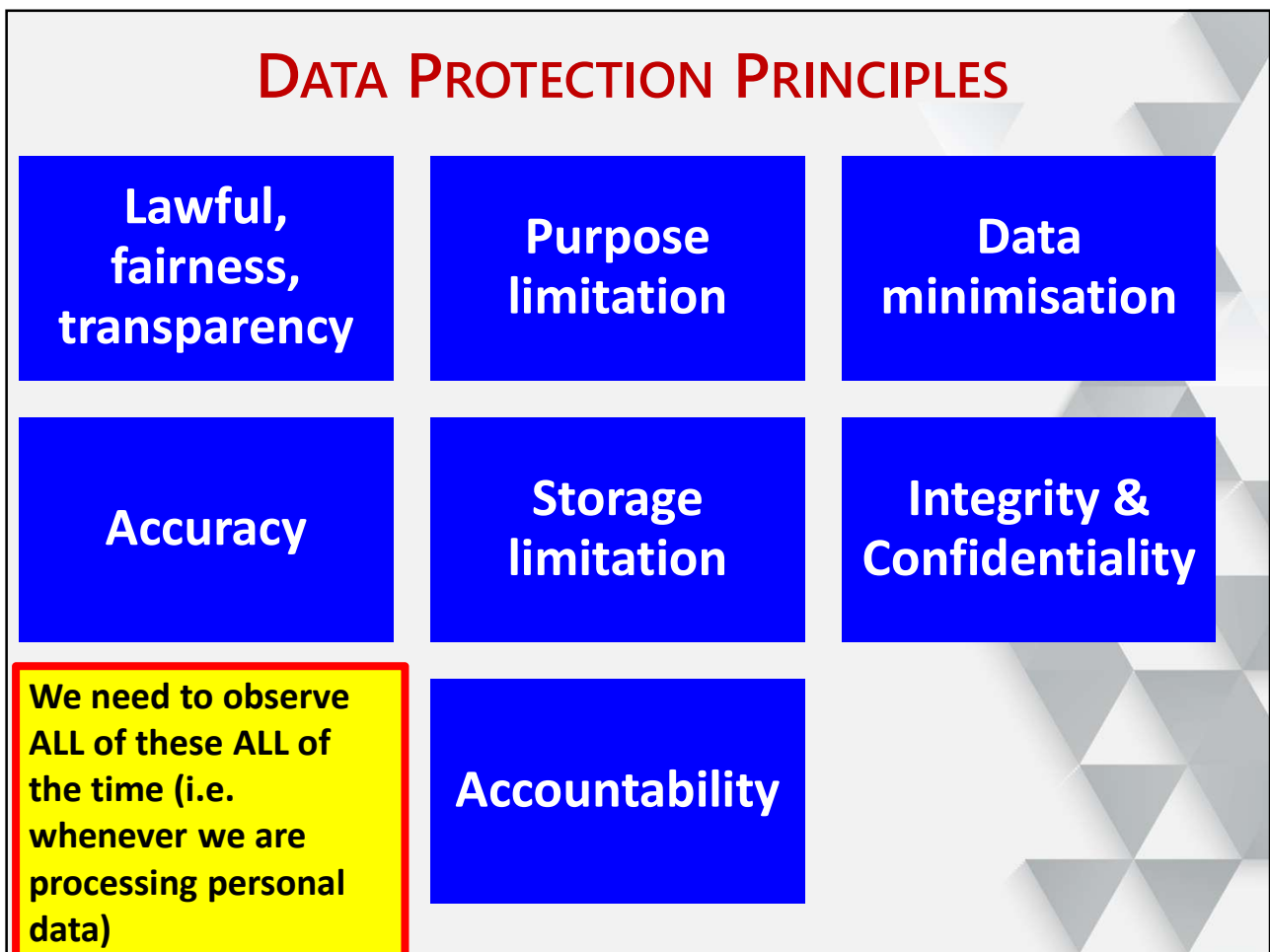
Rules... *statutory guidelines that controllers must follow...*

- Data Breach Records & Communications
- Privacy Notices/ Statements
- Data Processing Agreements
- Records of Processing Activities
- Risk Assessments
- Data Security Measures

www.jmb.ie

4

4

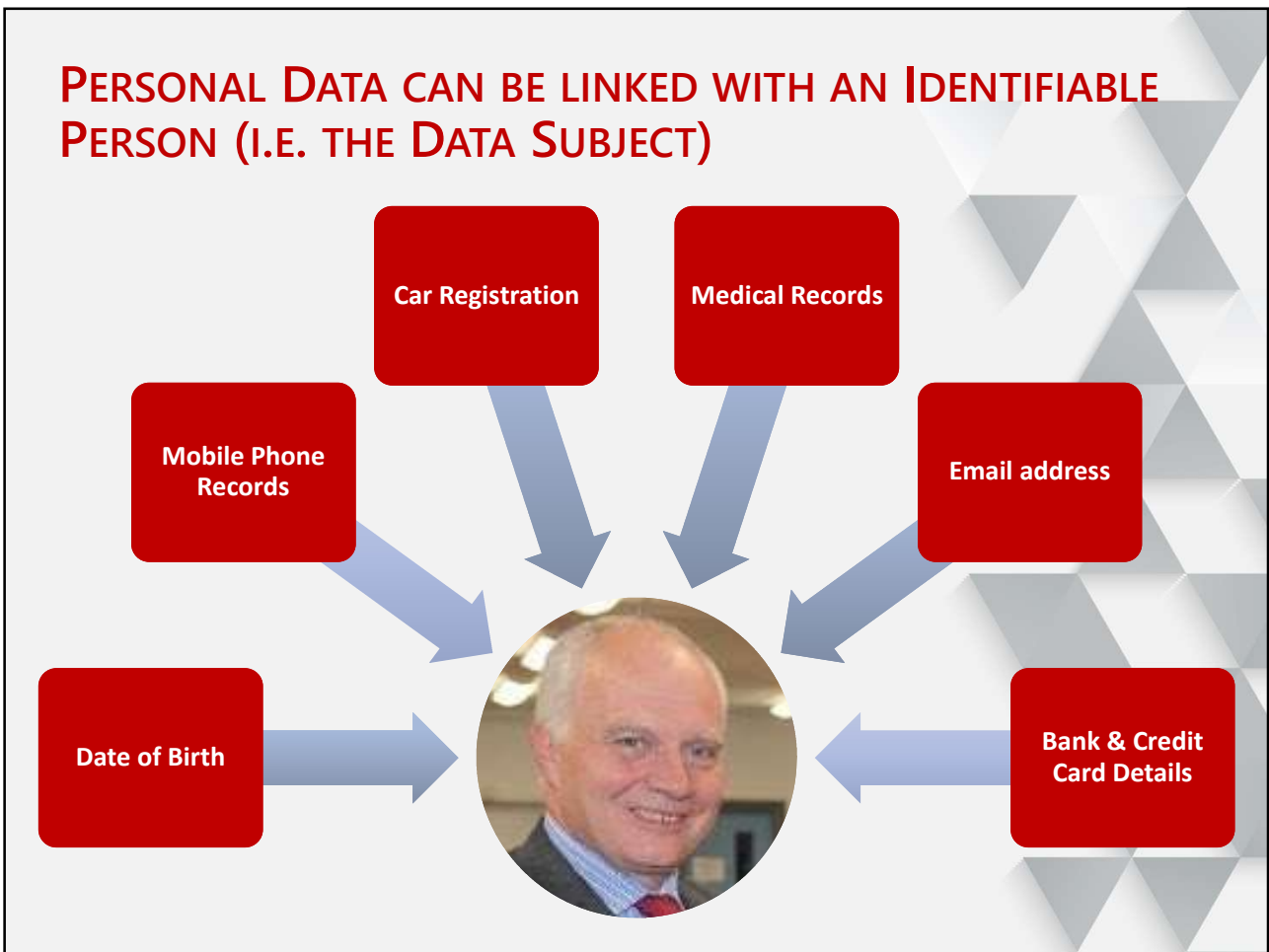


5

WHAT IS PROCESSING?

- **PROCESSING** is defined as ‘any operation or set of operations which is performed on personal data or sets of personal data, whether or not by automated means’.
- **PROCESSING** includes collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

6



7

Special Category Data

personal data that reveals (or has the potential to reveal):

- racial or ethnic origin,
- political opinions,
- genetic information,
- trade union membership,
- religious or philosophical beliefs,
- biometric information (where used to identify),
- health information
- information concerning sex life or sexual orientation.

**“Sensitive
Data”**

**e.g. take extra care
with medical and
SEN data**



Privacy Commissioner
Te Mana Mātāpono Matatapu

Ask

New Zealand

Case note 297084 [2019] NZPriv Cmr 11: Parents complain school mishandled their child's sensitive medical data

15 Oct 2019, 09:00

Two parents complained to our office after a primary school displayed their child's Medical Action Plan (MAP) in the school staffroom.

| | | |
|--------------------------------|--------------------|-----------------------------|
| Lawful, fairness, transparency | Purpose limitation | Data minimisation |
| Accuracy | Storage limitation | Integrity & Confidentiality |

9

9

GDPR example (1)

- a request asking the school to share pupil data is received from a public service body (e.g. Department of Education/ HSE)

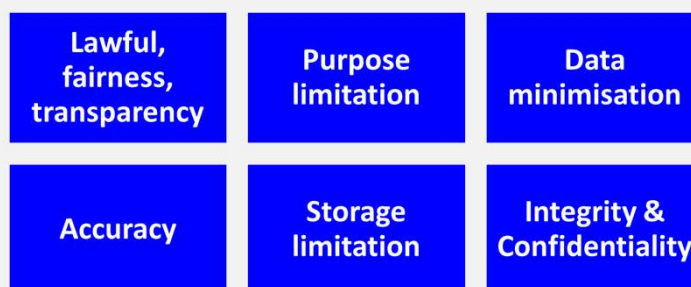
www.jmb.ie

10

10

GDPR example (2)

- a service provider is looking for access to parental data (e.g. a list of names & mobile telephone numbers)



11

11

GDPR example (3)

- a former staff member is seeking a copy of their file

www.jmb.ie

12

12

Teaching Council fined €60,000 after teacher data leaked in phishing scam Irish Examiner



The initial breach occurred when two council staff members opened a suspicious email, which facilitated the creation of an auto-forward rule allowing for emails to be forwarded from the council's servers to a malicious Gmail address.

13

13

Data Breaches in schools... examples



Non-use of BCC for email addressing

Letter / email sent to wrong person



data accessed via compromised cloud account

School records found in rubbish dump



School data destroyed

Ransomware attack



Personal Data Breach under GDPR?

CONFIDENTIALITY BREACH

- unauthorised or accidental **disclosure** of, or access to, personal data

AVAILABILITY BREACH

- accidental or unauthorised loss of access to, or **destruction** of, personal data


INTEGRITY BREACH

- unauthorised or accidental **alteration** of personal data

The Law changed on 25th May 2018

- Schools must keep a formal record of all personal data breaches
- Schools must report to DP Commissioner within 72 hours
 - unless unlikely to result in risk
- Schools must inform Data Subjects without undue delay
 - if likely to result to high risk to them

All staff need to: (i) recognise a personal data breach, and, (ii) report immediately to senior management




National Cyber Security Centre
a part of GCHQ




NCSC.co.uk

This advice has been produced to help small businesses protect themselves from the most common cyber attacks. The 5 topics covered are easy to understand and cost little to implement. Read our quick tips below, or find out more at www.ncsc.gov.uk/smallbusiness.

Backing up your data





Take *regular* backups of your important data, and test they can be restored. This will reduce the inconvenience of any data loss from theft, fire, other physical damage, or ransomware.



-  **Identify what needs to be backed up.** Normally this will comprise documents, photos, emails, contacts, and calendars, kept in a few common folders. Make backing up part of your everyday business.
-  **Ensure the device containing your backup is not permanently connected to the device holding the original copy, neither physically nor over a local network.**
-  **Consider backing up to the cloud.** This means your data is stored in a separate location (away from your offices/devices), and you'll also be able to access it quickly, from anywhere.


Preventing malware damage








You can protect your organisation from the damage caused by 'malware' (malicious software, including viruses) by adopting some simple and low-cost techniques.

-  **Use antivirus software on all computers and laptops. Only install approved software on tablets and smartphones, and prevent users from downloading third party apps from unknown sources.**
-  **Patch all software and firmware** by promptly applying the latest software updates provided by manufacturers and vendors. Use the 'automatically update' option where available.
-  **Control access to removable media** such as SD cards and USB sticks. Consider disabling ports, or limiting access to sanctioned media. Encourage staff to transfer files via email or cloud storage instead.
-  **Switch on your firewall** (included with most operating systems) to create a buffer zone between your network and the Internet.

Using passwords to protect your data


Passwords - when implemented correctly - are a free, easy and effective way to prevent unauthorised people from accessing your devices and data.








-  **Make sure all laptops, Macs and PCs use encryption products that require a password to boot. Switch on password, PIN protection or fingerprint recognition for mobile devices.**
-  **Use two factor authentication (2FA)** for important websites like banking and email, if you're given the option.
-  **Avoid using predictable passwords** (such as family and pet names). Avoid the most common passwords that criminals can guess (like *password*).
-  **Do not enforce regular password changes;** they only need to be changed when you suspect a compromise.
-  **Change the manufacturers' default passwords** that devices are issued with, before they are distributed to staff.
-  **Provide secure storage** so staff can write down passwords and keep them safe (but not with the device). Ensure staff can reset their own passwords, easily.
-  **Consider using a password manager.** If you do use one, make sure that the 'master' password (that provides access to all your other passwords) is a strong one.

Keeping your smartphones (and tablets) safe


Smartphones and tablets (which are used outside the safety of the office and home) need even more protection than 'desktop' equipment.






-  **Switch on PIN/password protection/fingerprint recognition for mobile devices.**
-  **Configure devices so that when lost or stolen they can be tracked, remotely wiped or remotely locked.**
-  **Keep your devices (and all installed apps) up to date, using the 'automatically update' option if available.**
-  **When sending sensitive data, don't connect to public Wi-Fi hotspots - use 3G or 4G connections (including tethering and wireless dongles) or use VPNs.**
-  **Replace devices that are no longer supported by manufacturers with up-to-date alternatives.**

Avoiding phishing attacks

In phishing attacks, scammers send fake emails asking for sensitive information (such as bank details), or containing links to bad websites.



-  **Ensure staff don't browse the web or check emails from an account with Administrator privileges.** This will reduce the impact of successful phishing attacks.
-  **Scan for malware and change passwords as soon as possible** if you suspect a successful attack has occurred. **Don't punish staff** if they get caught out (it discourages people from reporting in the future).
-  **Check for obvious signs of phishing, like poor spelling and grammar, or low quality versions of recognisable logos.** Does the sender's email address look legitimate, or is it trying to mimic someone you know?

© Crown Copyright 2017

For more information go to www.ncsc.gov.uk

Summary

- ❑ **Data protection is a whole school responsibility**
- ❑ **Respect the Processing Principles**
- ❑ **Extra care if it is sensitive data (e.g. SEN, medical, etc)**
- ❑ **Always check if / what / & how before sharing data**
- ❑ **Report any data breach to school management**
- ❑ **Thank you!**

www.jmb.ie



Reference sites

- JMB.ie (members section) e.g.
 - JMB Template Data Protection Policy
 - JMB Data Breach Procedure (& Recorded Webinar)
 - Risk management advice
- GDPR4schools.ie
- DataProtectionSchools.com
- DataProtection.ie
- GDPRandYOU.ie
- ICO.org.uk
- NCSC.co.uk