GDPR – top tips for compliance

Gill Dickson, Senior Policy Officer

27 November 2018

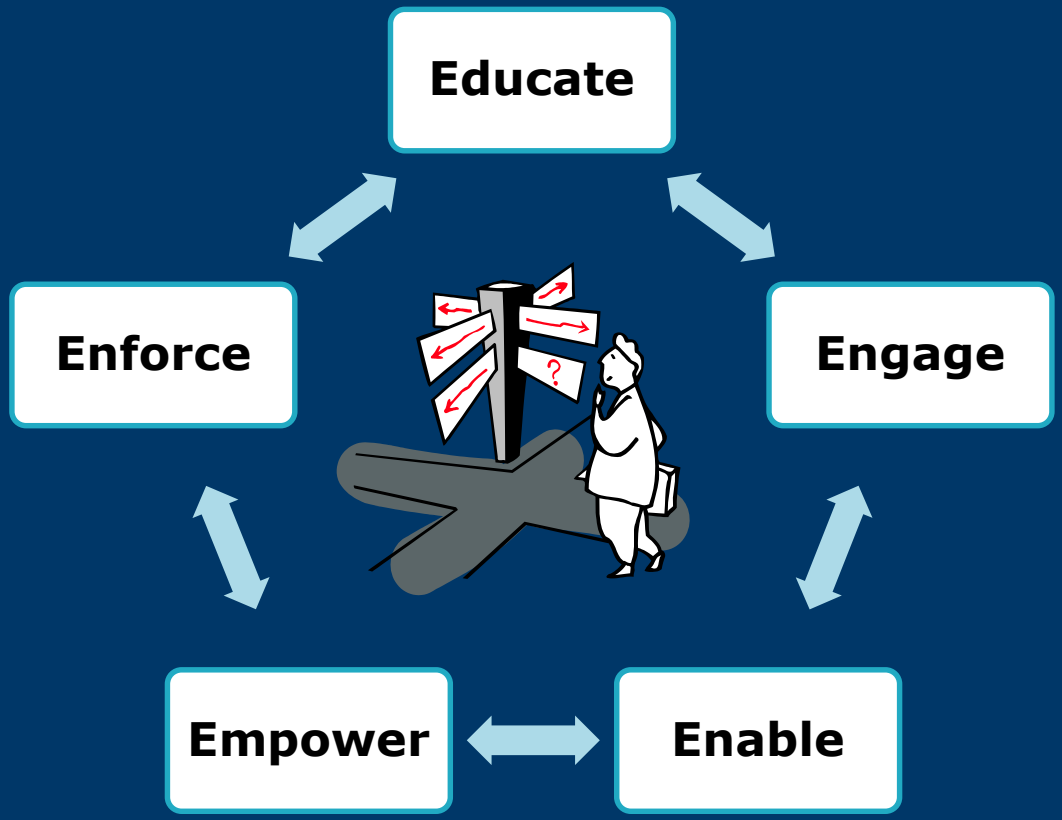
ico.
Information Commissioner's Office

Who we are

- The UK's independent body set up to uphold information rights
- Enforce and regulate freedom of information and data protection laws
- Provide information and advice
- Promote good practice

ico.
Information Commissioner's Office

The ICO's role



ico.
Information Commissioner's Office

25 M

ico.
Information Commissioner's Office

Impact: schools have been asking..

Subject access requests?

Who's the controller?

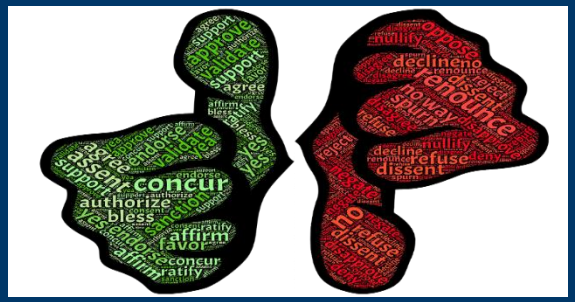
Can we disclose or display information?

What about third parties, such as educational apps and cashless catering?

Parent wants to erase all their data! Help!

ico.
Information Commissioner's Office

Lawful bases for processing



Consent

Contract

Legal Obligation

Vital Interest

Public Task

Legitimate Interest

ico.
Information Commissioner's Office

Since May 25...

- Over 300 complaints re education
- subject access requests are the most common
- the disclosure of data by organisations next
- The vast majority of incidents were cyber cases
- Almost half breaches were phishing attacks

ico.
Information Commissioner's Office

GDPR Principles

a) Lawfulness, fairness and transparency

b) Purpose limitation

c) Data minimisation

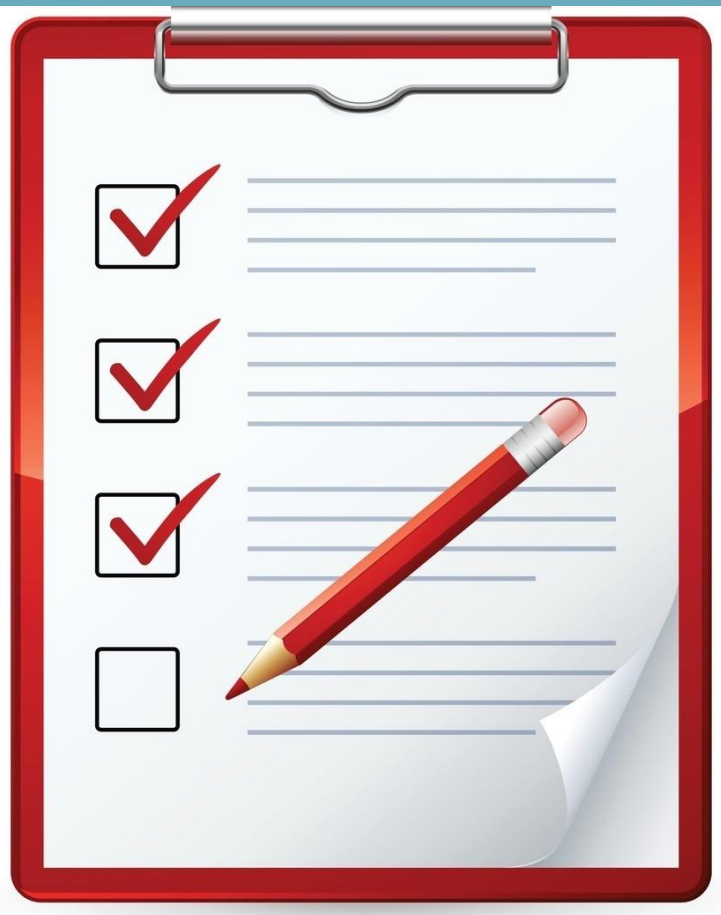
d) Accuracy

e) Storage limitation (retention)

f) Integrity and confidentiality (security)

g) Accountability

Can you show how you are complying with the law?



Information Commissioner's Office

Rights

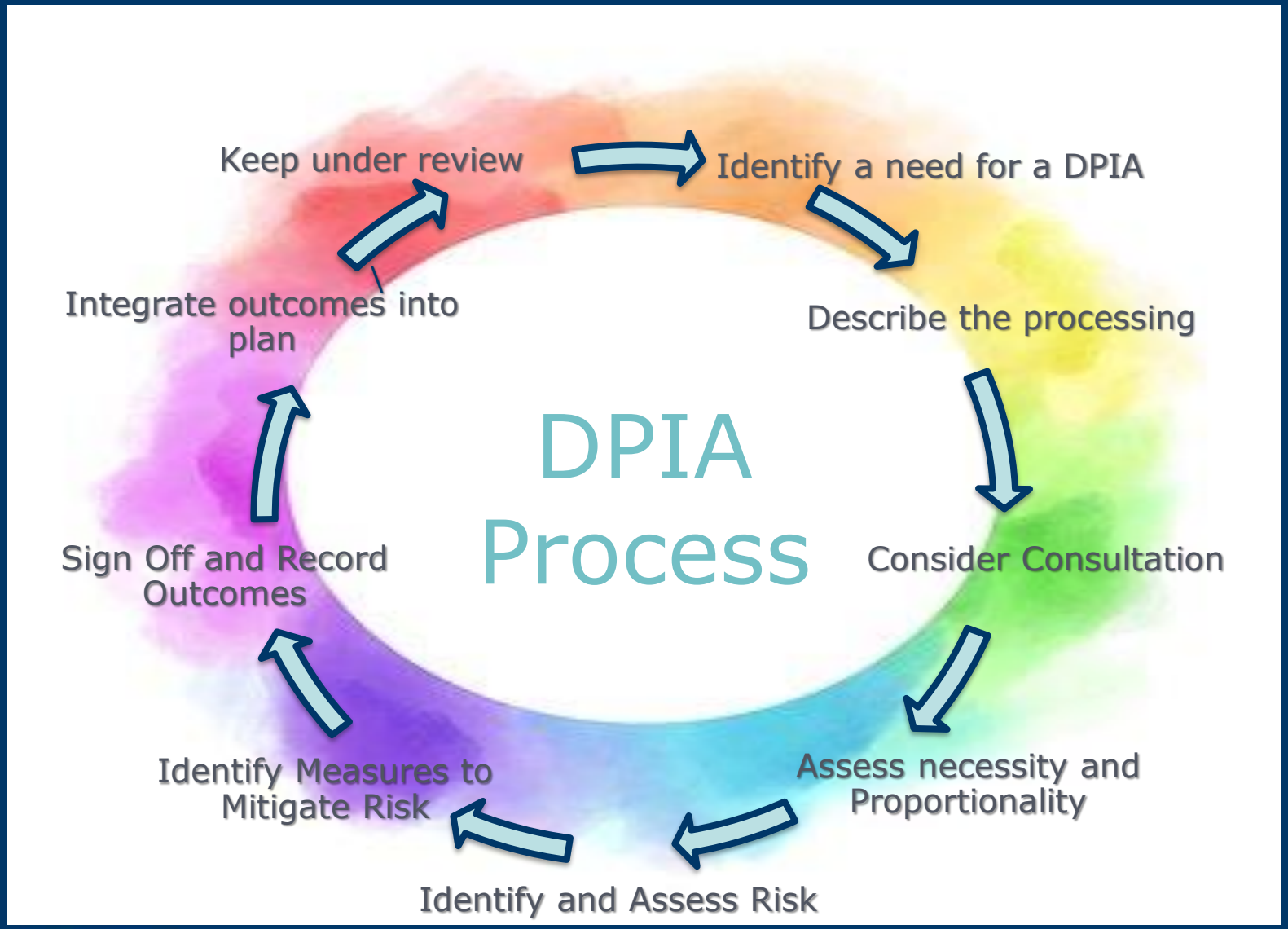
- Subject access requests
- Right to be informed
- Right to object
- Right to rectification
- Right to erasure
- Right to restrict processing
- Right to data portability
- Rights around automated processing

ico.
Information Commissioner's Office

Demonstrating accountability

- Data Protection Impact Assessments
- Data Protection Officers
- Contracts and Information Sharing Agreements
- Data protection by design and default

ico.
Information Commissioner's Office



ico.
Information Commissioner's Office

Data protection by design and default

ico.
Information Commissioner's Office


Breach
Notification
ico.
Information Commissioner's Office

Not every data breach needs to reported

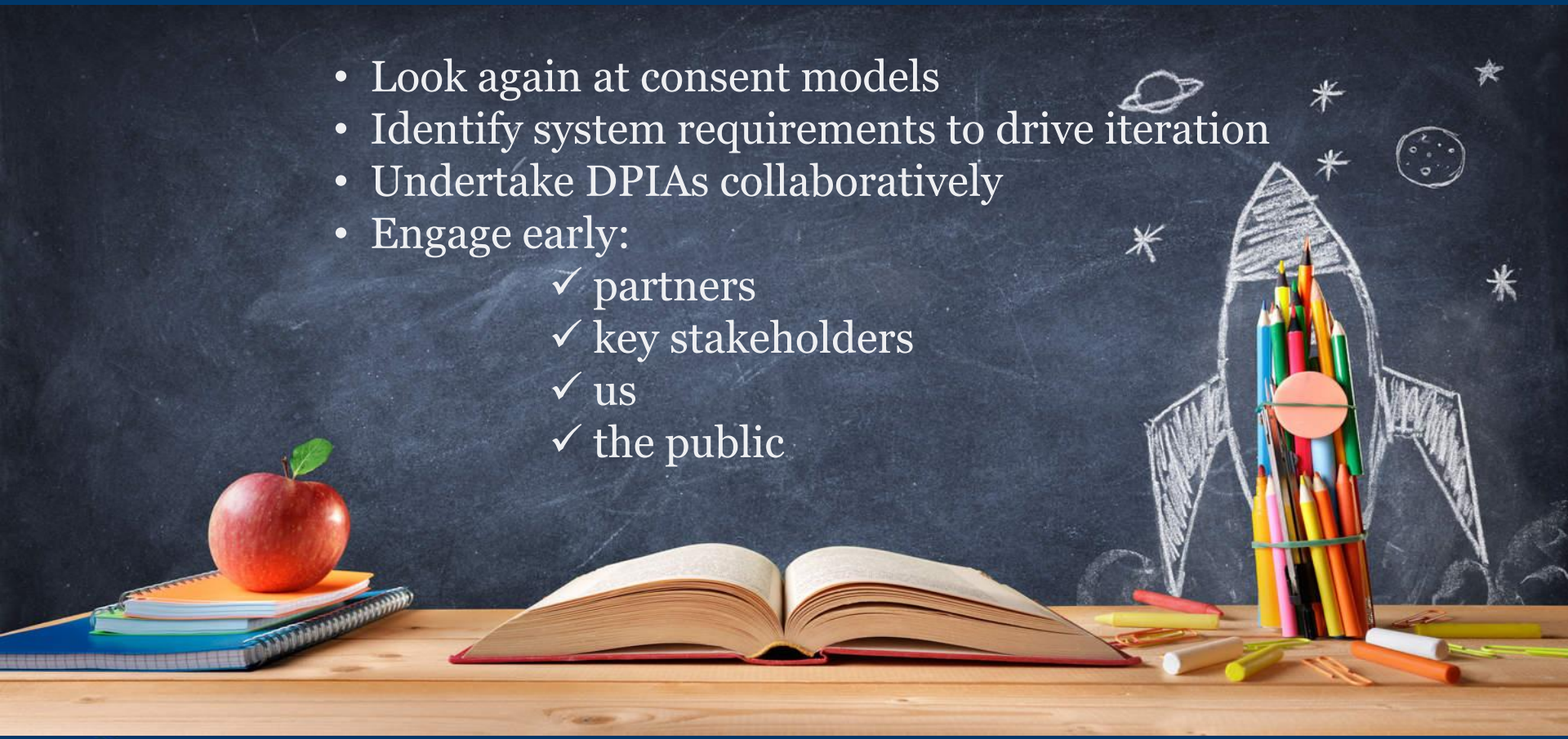
Best way to report a breach is over the phone

72 hours

- Only applies to personal data breaches as per the definition in GDPR (Art 4(12)
- Only reportable where it is likely there is a risk to people's rights and freedoms
- 72 hours – includes evenings/weekends/bank holidays (not just working hours)
- It is not a 72 deadline to just get in contact with the ICO - It's 72 hours, where feasible, to provide the information set out at Article 33 of the GDPR.
- **0303 123 1113 – Mon-Fri 9am-4:30pm**

ico.
Information Commissioner's Office

Emerging tips …



- Look again at consent models
- Identify system requirements to drive iteration
- Undertake DPIAs collaboratively
- Engage early:
  - ✓ partners
  - ✓ key stakeholders
  - ✓ us
  - ✓ the public

ico.
Information Commissioner's Office

Is this your biggest concern?

The ICO will issue a huge fine, won't they..?

Keep in touch

More than 100,000 people subscribe to our monthly e-newsletter: ico.org.uk/newsletter

ICO helpline: 0303 123 1113

Social media

@ICOnews

YouTube

Linked in