GDPR Preparation

for

Schools, Governors & Clerks

Pete Hutchings

Spring 2018

Bracknell Forest Council

Housekeeping

Is this what GDPR means?

News

Schools face hefty fines for data breaches under new EU laws

John Dickens| 5:00, Jul 3, 2017

Schools face having to free up a teacher to work three days every week on EU data protection issues, say tech experts.

Course objectives

- To understand the new General Data Protection Regulation (GDPR)
- To understand what you need to know and how it will affect your setting
- To understand the dual role of the Information Commissioner's Office (ICO)
- To consider the role of governors in preparation for and implementation of GDPR
- Stay awake!!

Data Protection… what you need to know

https://www.youtube.com/watch?v=jwFoMe5vE-o

Data Protection… what you need to know

- Who are the data subjects for schools?
- Who is the data controller?
- Who is the data processor?
- What examples of data are there in your setting?

Personal data & Sensitive Personal data

- The GDPR's definition of personal data is *"any information relating to an individual, whether it relates to his or her private, professional or public life. It can be anything from a name, a home address, a photo, an email address, bank details, posts on social networking websites, medical information, or a computer's IP address."*
- The GDPR refers to sensitive personal data as "special categories of personal data". These categories are broadly the same as those in the DPA, but there are some minor changes, e.g. the special categories specifically include genetic data, and biometric data where processed to uniquely identify an individual.

Legislative position

- UK Data Protection Act 1998 (**DPA**)
- General Data Protection Regulation (**GDPR**)
  - applies from 25 May 2018
  - the government has confirmed that the UK's decision to leave the EU will not affect the commencement of the GDPR
- Guidance being regularly updated by the EU's Article 29 Working Party
- Data Protection Bill currently with Parliament

Data Protection Act 1998

ARTICLE 29
Data Protection Working Party

ico.
Information Commissioner's Office

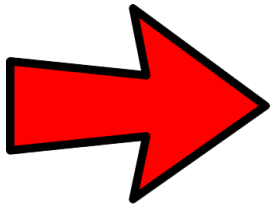
- Independent body set up to uphold information rights
- Enforce and regulate freedom of information and data protection laws
- Provide helpful information and advice
- Promote good practice
- Check your registration
  https://ico.org.uk/esdwebpages/search

ico.
Information Commissioner's Office

Data protection fee

- Annual fee payable from registration renewal date
- Likely to be £60 (Tier 2)
- ICO will write before renewal to remind and tell you what tier you are
- Will collect information from you and publish most of it
  - Name and address of data controller (school)
  - Number of staff (and turnover)
  - Level of fee and date paid
  - DPO contact details (name may be withheld)
- For full details see here

DPA Principles



GDPR Principles

- Be processed fairly and lawfully
- Be obtained for specified and lawful purposes
- Be adequate, relevant and not excessive
- Be accurate and kept up-to-date
- Not be processed for any purpose, shall not be kept for longer than is necessary
- Be processed in line with the rights of data subjects
- Be secure and protected against unauthorised or unlawful processing, loss destruction or damage
- Not be not be transferred to any country without adequate protection

- Processed lawfully, fairly and in a transparent manner
- Collected for specified, explicit and legitimate purposes
- Adequate, relevant and limited to what is necessary
- Accurate and kept up-to-date
- Kept in a form which permits identification of data subjects for no longer than is necessary
- Processed in a manner that ensures appropriate security, including protection against unauthorised or unlawful processing, accidental loss, destruction or damage

https://www.knowyourcompliance.com/beginners-guide-to-the-general-data-protection-regulation-gdpr/

Implications of GDPR

- Same basic principles as current DPA, but strengthened
- Greater accountability for data controllers, i.e. schools
- Increased rights for data subjects, i.e. parents and children
- Increased requirement to be able to demonstrate compliance
- New requirements for breach reporting
- Use of Data Protection Impact Assessments (DPIAs)
- Higher penalties for non-compliance

Compliance

- Requirement to implement appropriate technical and organisational measures
- Maintaining records on processing activities
- Utilise, as appropriate, Data Protection Impact Assessments (DPIAs)
- Requirement to appoint a Data Protection Officer
- Data protection by ‘Design & Default’
- Keep an ‘Information Asset Register’

Data Protection Officer

- Do we have to have one?
- Requirements for the role:
  - inform and advise
  - monitor compliance, advise on DPIAs, train staff and conduct internal audits
  - be the first point of contact
- DPO must…
  - report to the highest management level
  - operate independently and cannot be dismissed or penalised for performing their task
  - be enabled to do the job, e.g. resources & training

Data Protection Officer

- Conflicting advice!
- Make a **reasoned** choice
- Beware conflicts of interest
- External providers available but at a cost
- So who should it be and how do you best protect them in their role?

Some observations/advice:

- https://www.gdpr.school/who-will-be-your-schools-dpo/
- https://dataprotection.education/blog/18-gdpr-in-education/23-the-gdpr-and-your-school-the-data-protection-officer-dpo
- https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/accountability-and-governance/data-protection-officers/ (Most helpful)

Data breaches

- Most common ones in education:
  - Lost/stolen paperwork or unencrypted computers and memory sticks
  - Data posted/faxed or e-mailed to the incorrect recipient
- ICO maintains a list of all breaches and analyses reporting trends
- New requirements under GDPR for reporting and disclosure:
  - In the case of a personal data breach the ICO must be notified without undue delay and where feasible not later than 72 hours after the breach was discovered.
  - Must inform the person if the breach puts their rights and freedoms at high risk (for example the leak of personally identifiable data).
  - Increased fines – up to €20 million or 4% of annual global turnover!

Privacy notices (for pupils, parents, staff and governors)

- What data is collected about them?
- What purpose(s) the data is being collected for?
- How will the data be used (processed)?
- What is the lawful basis for processing?
- How long is the data retained for?
- Who will the data be shared with?
- Why is the data shared?

DfE model documents for pupils, parents and staff:

https://www.gov.uk/government/publications/data-protection-and-privacy-privacy-notices

Privacy notices & GDPR

- Concise, transparent, intelligible and easily accessible
- Written in clear and plain language, particularly if addressed to a child
- Free of charge
- See ICO code of practice
- See ICO Checklist

GDPR & Consent

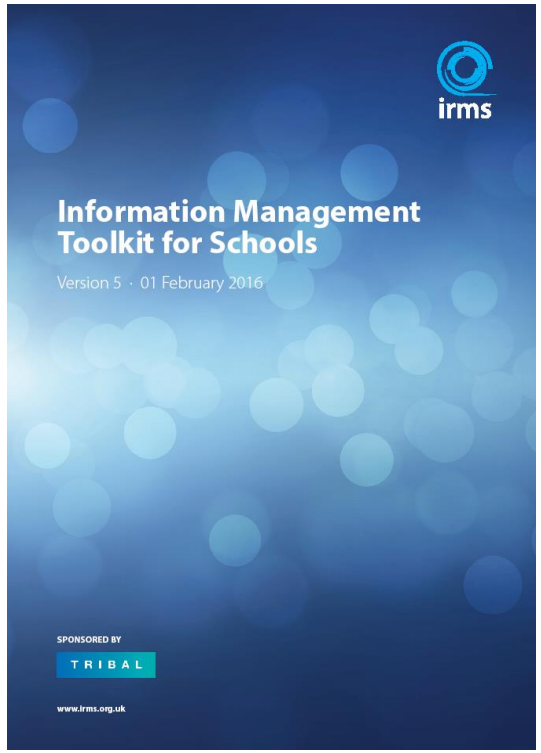
- Conditions for this have been strengthened
- Requests for consent must be in an *“intelligible and easily accessible form, using clear and plain language”*
- Requests for consent must also include the purpose for the data request
- Must be as easy to withdraw consent as to give it
- Giving consent must be a positive action (not pre-ticked box)
- Only need consent where another lawful basis does not apply

Data transfer, deletion and disposal

GDPR is about minimising data retention times

- What data can/should you delete?
- When may you do this?
- How will you do this?
- What about pupil transfers to another school?
- Follow ‘local’ rules/guidelines
- Comprehensive guidance available from **IRMS**:

  http://irms.org.uk/page/SchoolsToolkit



Security of data

Personal data shall be…

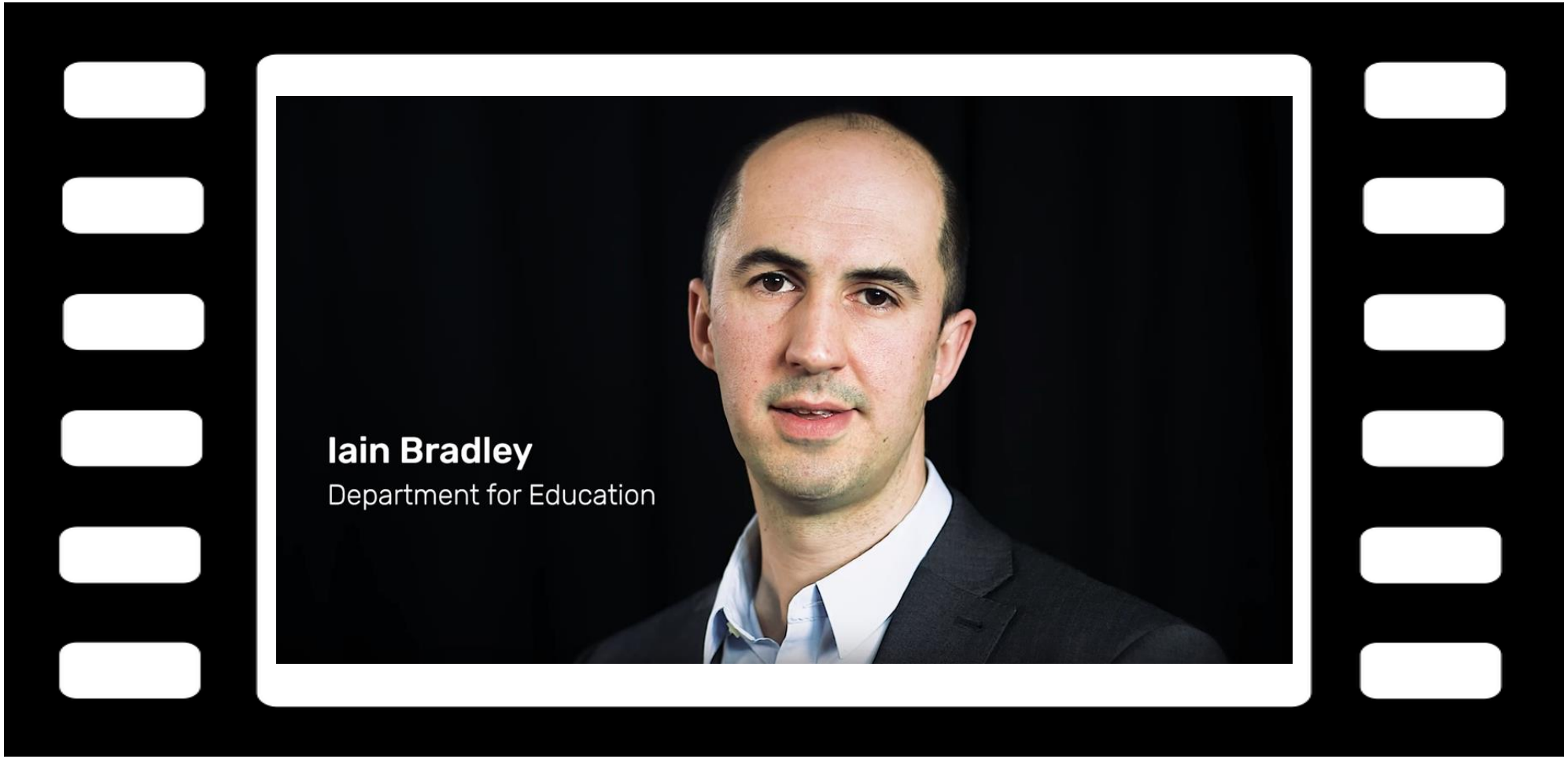
*“processed in a manner that ensures **appropriate security** of the personal data, including protection against **unauthorised or unlawful** processing and against **accidental** loss, destruction or damage, using appropriate **technical or organisational** measures.”*

GDPR - Article 5(f)

Data Security

- Strong password policy (https://howsecureismypassword.net/)
- Multi Factor Authentication if possible
- Encryption – USB sticks, drives, laptops, mobiles, BYOD
- User training - Phishing and ransomware
- Data and Device Disposal
- Joiners & Leavers
- See additional handouts

GDPR Guidance for Schools (DfE)



https://www.youtube.com/watch?v=y09IHXv6u6M&sns=em

Recent findings from the ICO

- Need for data protection training (at least every 2 years)
- Documented procedures should be in place for
  - managing security incidents
  - subject access requests
  - sharing data
  - data retention and deletion (paper and electronic)
- Other areas to ensure
  - individual and strong passwords
  - secure printing
  - clear policy/procedures for remote or homeworking
  - paper file security, e.g. clear desk policy
  - Immediate removal of access when staff leave

How to prepare for GDPR

- Policy & Procedures
  - Be accountable
  - Review all relevant current policies and procedures
  - Determine how you will react to a data breach
- Consent
  - Review and revise consent forms
  - Review and revise privacy notices
  - Ensure clear procedures for data deletion and requests for data erasure
- Data Processors
  - Ensure external data processors are compliant

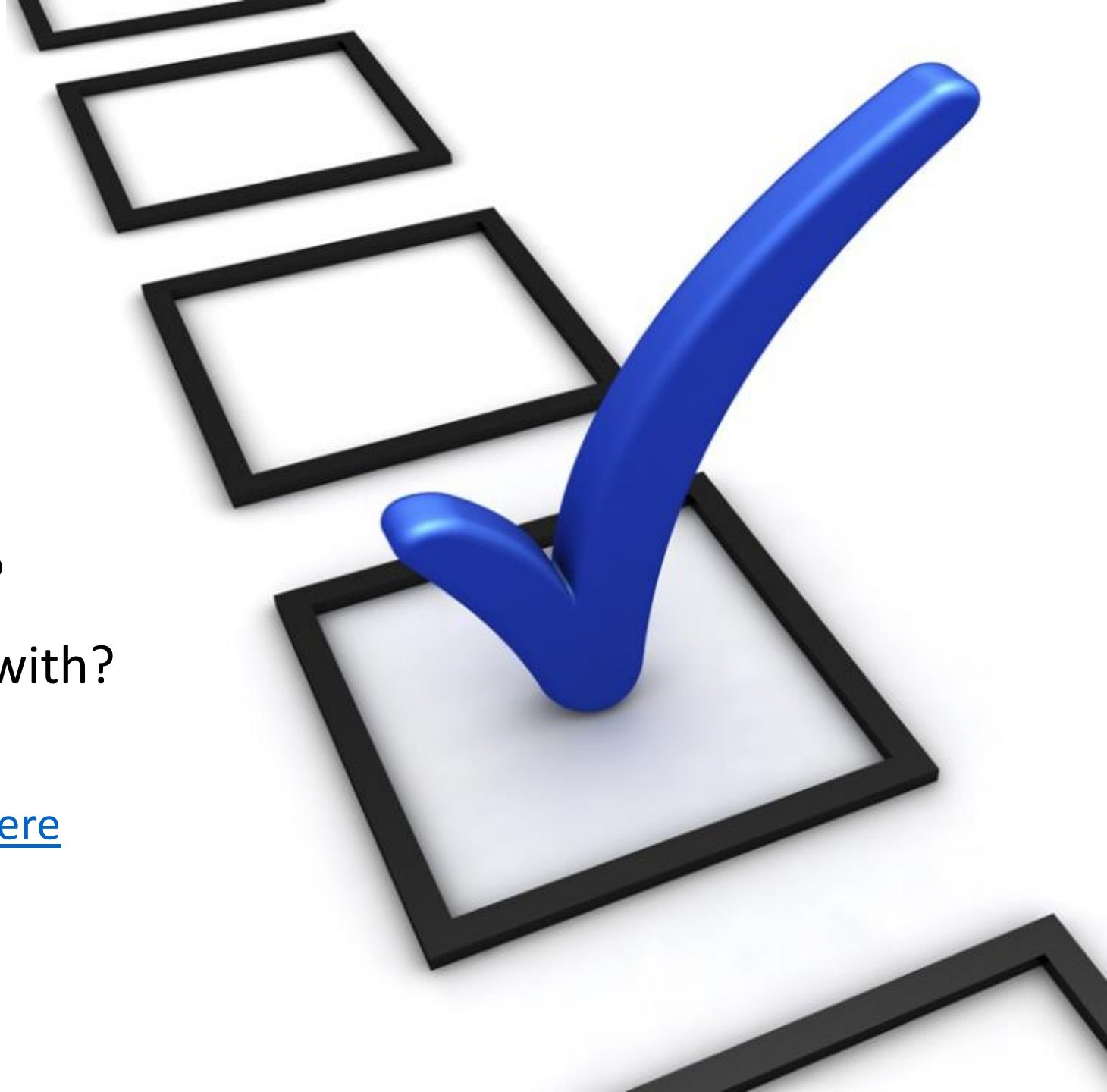
Getting ready for GDPR

- There are a number of self-assessment tools available:
  - ICO
  - Microsoft
  - GDPR in Schools
- Note any areas that may need:
  - Clarification
  - Action

Data audit

- What data do you collect?
- What is it used for?
- What is the legal basis?
- Who has access to the data?
- Who do you share the data with?

Sample data audit form available here



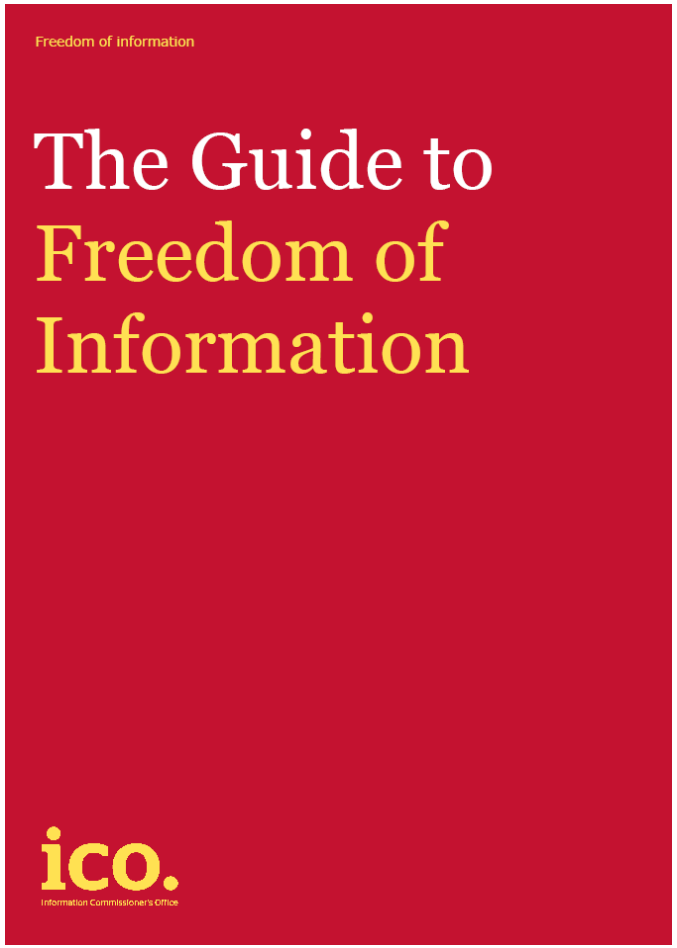
Subject Access requests

- Enables **individuals** to find out what personal data you hold about them, why you hold it and who you disclose it to
- Clear guidelines:
  - One month time limit, no charge
  - Confirm identity of requestor
  - Protect information about other people
  - Ensure response is clear and understandable
- Helpful online ICO checklist at

  https://ico.org.uk/for-organisations/subject-access-request-checklist/

Freedom of Information (FOI)

- School must produce a publication scheme, which outlines the information that is routinely made available.
- FOI requests:
  - Must be in writing with applicant's contact details
  - 20 school days to respond
  - May charge cost of copying and postage
  - May ask for clarification (20 days start once this is received)
  - Clear guidance of when a request may be refused



https://ico.org.uk/media/for-organisations/guide-to-freedom-of-information-4-9.pdf

Capita SIMS and GDPR

- Autumn release – new Person Data Output report to aid with Subject Access Requests for pupil information
- Spring release – PDO report for staff
- Developing means of selective data deletion where possible
- See recent Webinars
- For the latest information:
  - https://myaccount.capita-cs.co.uk/hot-topics/sims-gdpr/
  - https://myaccount.capita-cs.co.uk/hot-topics/SIMS-Parent-Lite/

What to do next

- Establish GDPR ‘team’ in schools to review and document compliance
- Do an audit of data and processes
- Review privacy notice, data collection process, lawful basis
- Obtain positive consent where necessary
- Review data protection policies, update staff education
- Establish and record GDPR compliance of 3rd party processors
- Review physical and electronic security policy and processes
- Update process for SARs, FOI, data breaches, new projects
- Appoint Data Protection Officer (DPO)

What should governors be doing?

- Keep things in proportion!
- Appreciate that this involves an increase in workload
- Understand and decide how best to tackle GDPR in your school
- Understand your personal responsibilities
- Designate a link governor
- Monitor GDPR compliance

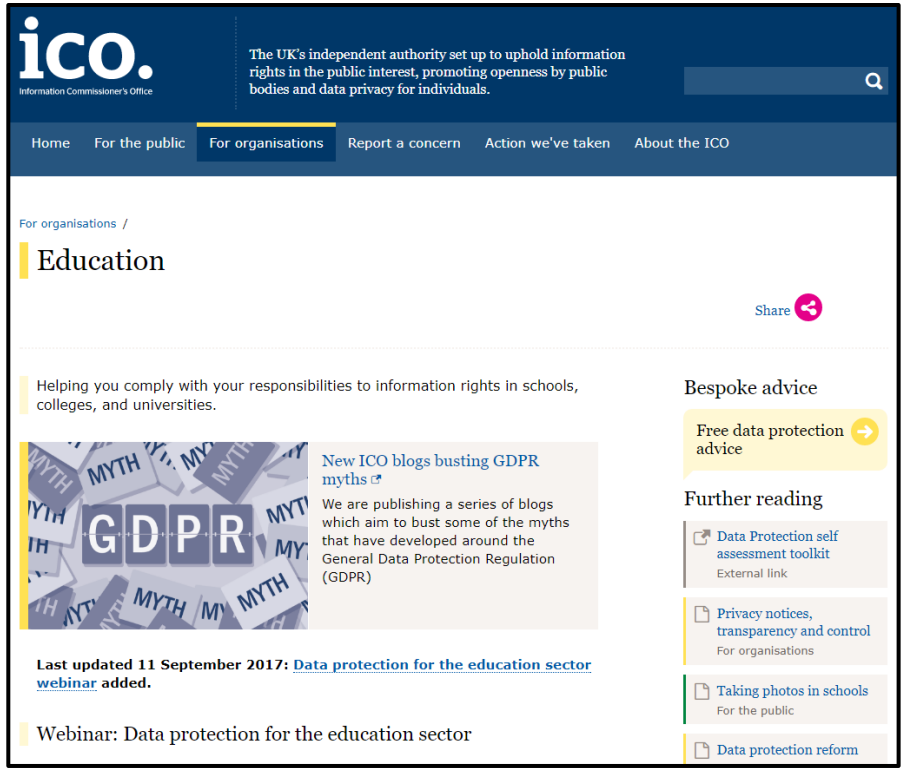
Summary (DPA)

https://vimeo.com/98420886

Evaluation form

Please complete before leaving

Further help



https://ico.org.uk/for-organisations/education/

ico. Information Commissioner's Office

frequently asked QUESTIONS

Data Protection and GDPR

Please refer to the Information Commissioner's Office (ICO) website for full information on Data Protection and Freedom of Information requests with regard to schools and educational institutions.

Useful information

- DfE Statutory guidance on policies for schools (2014) - covers Data Protection
- ICO Advice on processing children's data
- IRMS Records Management Tool Kit for Schools (2016) – contains detailed guidance on retention of data

General Data Protection Regulation (GDPR)

From 25 May 2018 schools will need to be compliant with the new legislation. Links to information, resources and tools that schools may find useful in making preparations are listed below.

General guidance on GDPR

- Information Commissioner's Office
- National Governors Association
- London Grid for Learning (LGfL) – select GDPR from the dropdown Topic menu
- Times Education Supplement

Webinars and Blogs

- DfE
- Browne Jacobson
- Optimus Education GDPR BLOG

Checklists and action plans

- ICO Preparing for GDPR (12 steps to take now)
- ICO Checklist for Data Controllers

In this section:

http://schools.bracknell-forest.gov.uk/policies-guidance/data-protection-and-gdpr