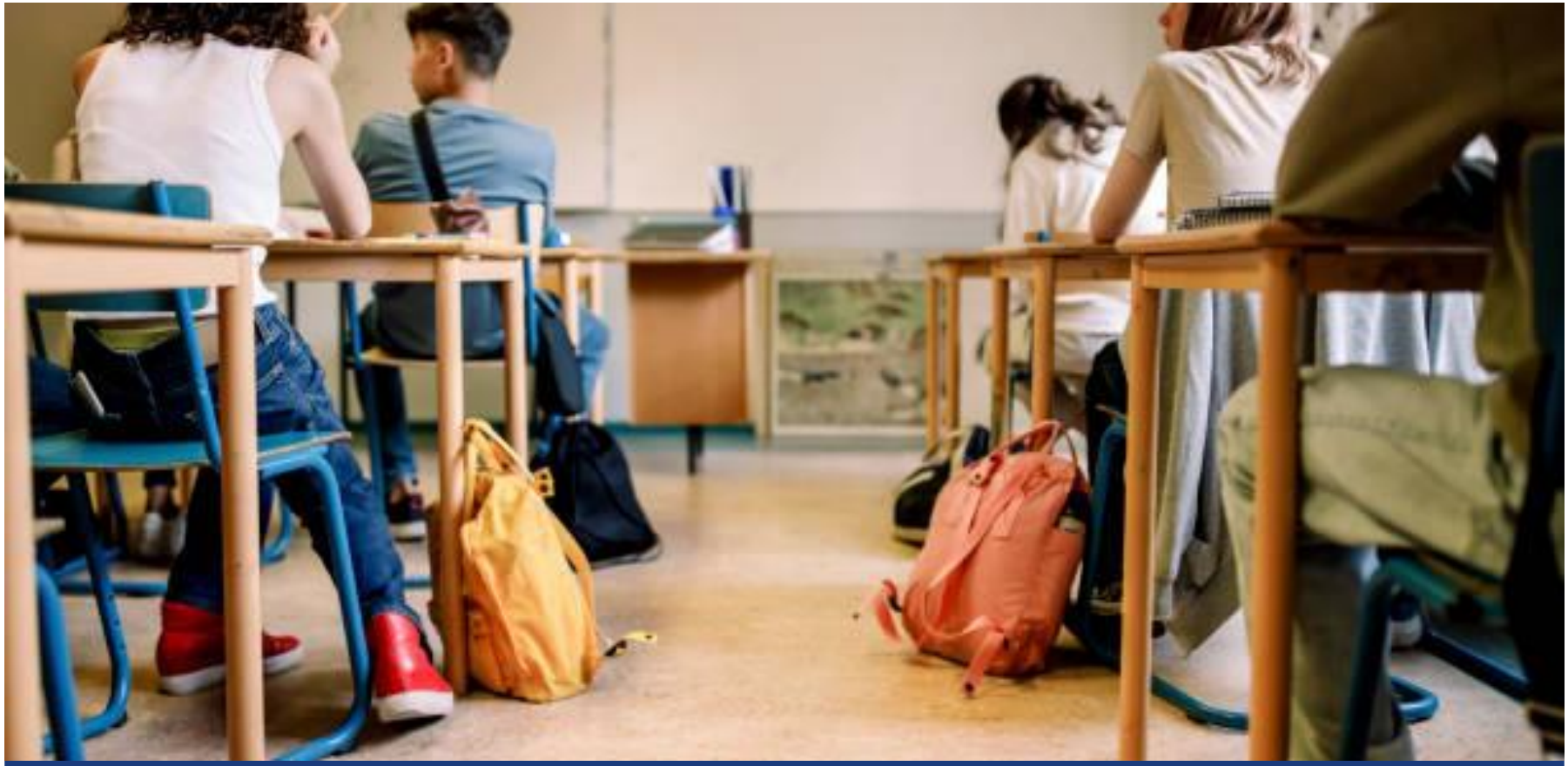


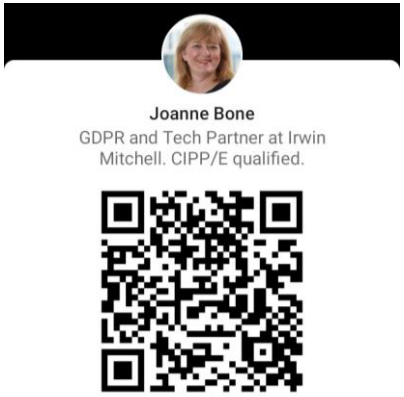
GDPR for the Education Sector: What to expect in 2023

England Rugby

Official Legal Partner

irwinmitchell

Your Speakers



Joanne Bone
Partner
Joanne.bone@irwinmitchell.com

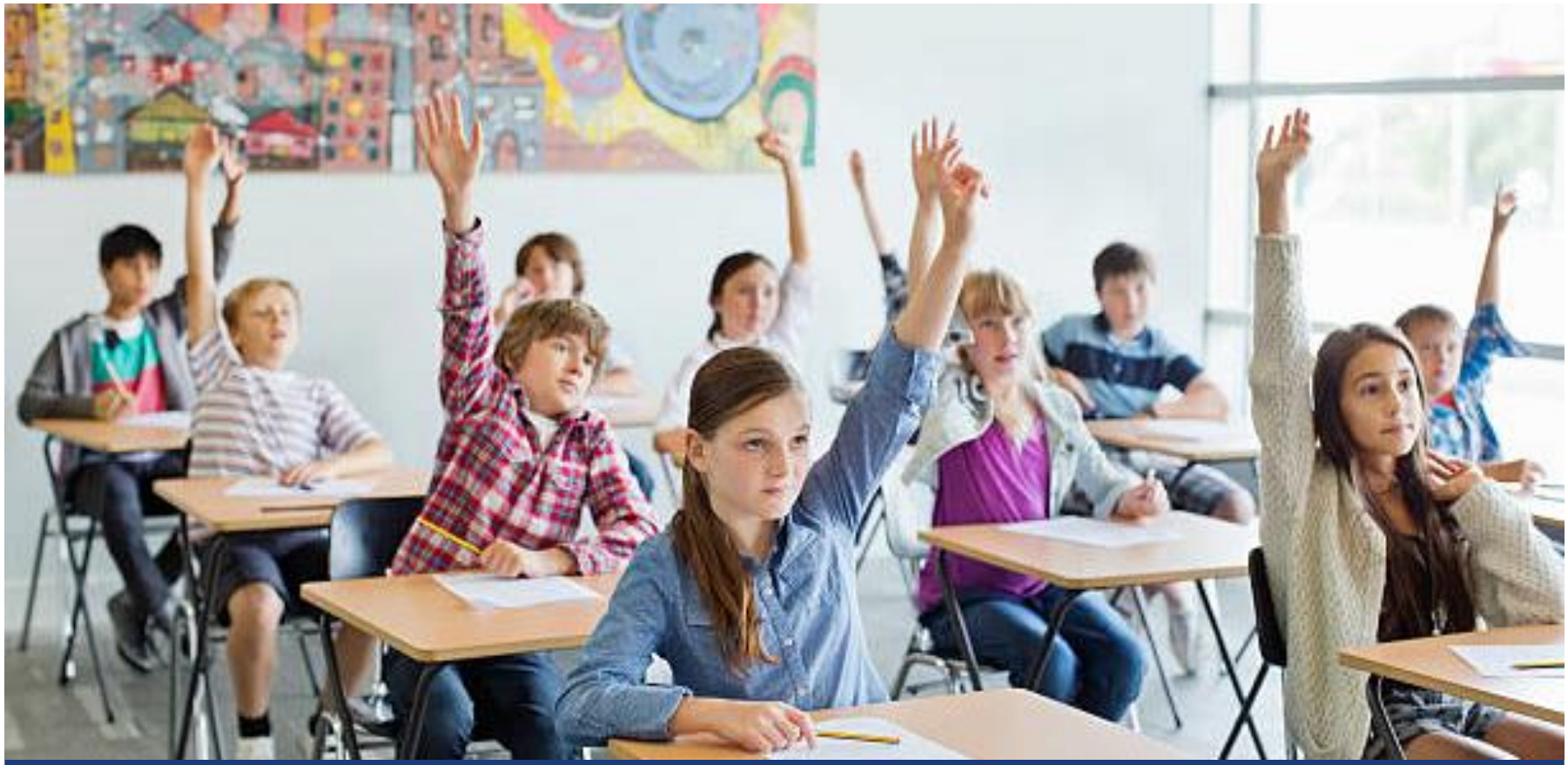
Hannah Moran
Solicitor
Hannah.moran@irwinmitchel.com

England Rugby
Official Legal Partner

IM irwinmitchell

What are we covering today?

- Recent guidance from the Department for Education
- What is the ICO interested in? “ICO25” Strategy and Enforcement
- What fines have been issued and for what?
- What is on the horizon? Data Reform Laws



Department for Education – Data Protection in Schools

England Rugby

Official Legal Partner

irwinmitchell

Data Protection in Schools: Guidance

- New DfE guidance published **3rd February 2023**

https://www.gov.uk/guidance/data-protection-in-schools

- The guidance aims to help schools and multi-academy trusts understand
  - What data protection means for schools
  - The lawful grounds for processing personal data
  - Who is responsible for data protection and what their role is
  - The appointment and role of a DPO
  - Policies and procedures
  - Sharing personal data
  - DSARs and other rights
  - Data retention
  - Managing breaches of data

Roles and Responsibilities

- The guidance sets out who is responsible for what part of data protection compliance:
  - **Governors and trustees**:
    - monitoring the schools data protection performance
    - supporting the data protection officer
    - ensuring a good network security infrastructure to keep personal data protected in place
    - Making sure there is a business continuity plan in place that includes cyber security
  - **Senior leaders:**
    - Decide on the uses of technology and how to maintain security
    - Decide what data is shared and how (making sure contracts with processors are UK GDPR compliant)
    - Assuring the right policies and procedures are in place
    - Making sure staff receive annual training
  - **Staff:**
    - Be aware of what ‘personal data’ and ‘processing’ means
    - Understand their duties and the processes in handling personal data
    - Understand their responsibilities in recognising and responding to a data breach
    - Be aware of the process is for recognising and escalating DSARs etc.

Special category data and criminal offence data

- Special category data under Article 9 of UK GDPR includes:
  - racial or ethnic origin
  - political opinions
  - religious or philosophical beliefs
  - trade-union membership
  - genetic information
  - biometric information (for example, a fingerprint)
  - health matters (for example, medical information)
  - sexual matters or sexual orientation
- The guidance advises that it is best practice to also treat the following as special category data :
  - safeguarding matters
  - pupils in receipt of pupil premium
  - pupils with special educational needs and disability (SEND)
  - children in need (CIN)
  - children looked after by a local authority (CLA)
- This expands upon the requirements of the law

Use of Consent

The guidance sets out advice on where consent should be used and who should give it

- **Fundraising and marketing:**
  - Complex area and method of contact is relevant – electronic marketing is more regulated
  - Where contact is via e.g. email – GDPR and PECR apply
  - Consent will be needed for fundraising
  - The guidance says that consent should be used for email marketing e.g. about a local holiday club
  - Legitimate interest/soft opt-in may be used for marketing (but not fundraising) by independent schools
- **Photographs:** the guidance says that schools have a legal obligation to seek consent to use pupil photographs (more on this later)
- **Data sharing:** the guidance says that before sharing any personal data, usually consent from the individual is required – but often data is shared without consent in practice

Use of Consent

- Situations where consent is not required (according to the guidance):
  - The individual cannot give it
  - It is not reasonable to ask for it
  - When there is a safeguarding concern
- There are other situations where consent is not generally required
- ICO data sharing code

Use of Consent

- **Who should give consent?**
  - The guidance says that usually a parent/someone with parental responsibility should give consent for pupils under 13 and the pupil themselves if they are over 13
  - It is more nuanced than that and depends upon the understanding of the child
- **Issues to bear in mind with consent:**
  - Consent must be freely given, granular, informed and unambiguous
  - Do not use pre-ticked boxes
  - Be clear and transparent about what the individual is agreeing to
  - Explain what personal data will be shared, who it will be shared with and how they will use it
  - Explain how it will be shared
  - A clear and easy process to withdraw consent should be given
  - The guidance says that you should include any relevant privacy notice
  - You must be really clear when asking consent from a pupil and write it in a way they can understand

Taking and Using Photos

- Consent is required for any use of a photograph, including to:
  - share photos on your school's social media channels
  - include photos of pupils and staff in your prospectus or other marketing material
  - use a photo of a pupil in your school displays
  - take a photo for a newspaper article

- Current ICO guidance is less restrictive than this
- Do not include the name of the pupil unless you have specific consent to do so
- The photo can only be used in line with the consent provided and for the time frame specified
- Photos used in identity management systems should be deleted when a child is no longer a pupil at the school

Publishing Exam Results

- Consent of the pupil, parent/those with parental responsibility is NOT required in order to publish results online or in the local press
- You should, however, tell pupils where and how their results will be published before they're published
- Give pupils an opportunity to ask you to remove their results from the list should they wish to

Data Protection Officer

- UK GDPR imposes a requirement on public authorities to appoint a DPO
- Private organisations have a choice and are only required to appoint one where:
  - your core activities require large scale, regular and systematic monitoring of individuals (for example, online behaviour tracking); or
  - your core activities consist of large scale processing of special categories of data or data relating to criminal convictions and offences.
- The new guidance states that schools/MAT **must** appoint a DPO
- UK GDPR requires that a DPO is independent:
  - i.e. They cannot determine the objectives and methods of data processing activities (e.g. IT director, HR, Marketing manager)
- The DPO can cover more than one school or MAT to share documents, resources and the burden on data protection compliance

DPIAs

- UK GDPR sets out a DPIA must be carried out where a type of processing is likely to result in a high risk to the rights and freedoms of individuals:
  - Systematic and extensive profiling
  - Large scale use of sensitive data
  - Public monitoring
- New DfE guidance highlights a DPIA is required where processing:
  - affects “vulnerable data subjects”: **children** (age), **employees** (power imbalance), **other vulnerable sectors** (with special protections)
  - involves “innovative technologies”: **biometrics, AI, IOT, safeguarding equipment**
- This is more onerous than ICO requirements
- There is no definitive format (although a ICO template is available) and it does not have to demonstrate that all risks have been eliminated, but it’ll help you document them and assess whether any that remain are justified.

Data Subject Access Requests (DSARs)

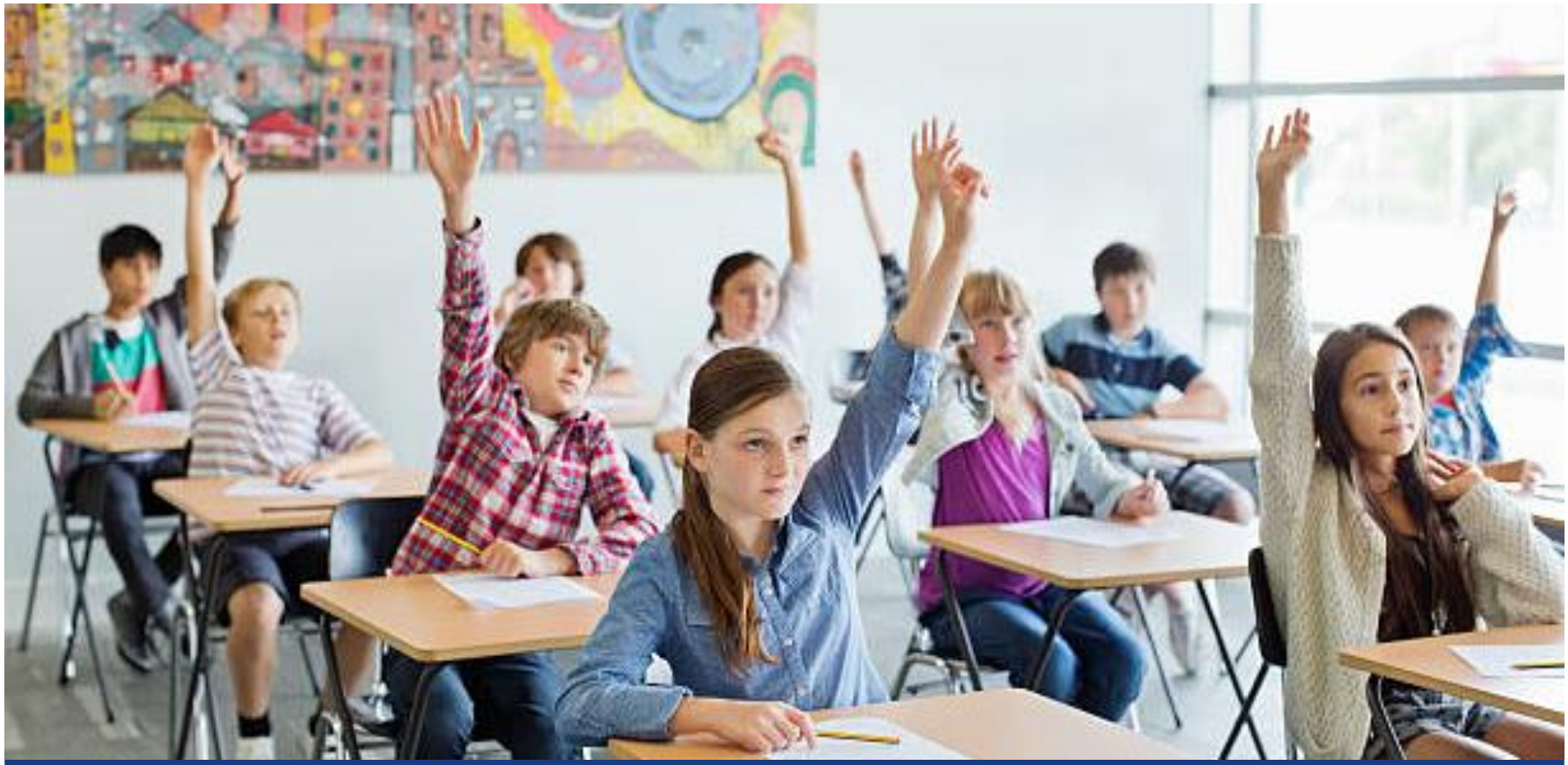
- DSARs normally come from: a pupil, a parent or carer (about themselves or child), staff, former staff/pupils, or solicitors on their behalf.

- The DfE's guidance sets out the scenario where a parent makes a request on behalf of a child and takes the approach that:

  1. provided the child is under 13, the requester with parental responsibility may make the DSAR on behalf of the child, or
  2. provided the child is aged 13 or older, they must have given their consent for the parent or carer to act on their behalf

- It is not one-size fits all and a child aged 13 or older must still be competent and acting in their best interests.

  - You must assess the child's level of maturity and that they understand what they are asking for and will receive in broad terms, or that they understand the consequences of authorising someone else
  - If the child is deemed competent you should respond directly to them



What is the ICO interested in?

England Rugby

Official Legal Partner

irwinmitchell

What is the ICO interested in? Strategy

The ICO launched “ICO25” setting out its strategic objectives for the next 3 years:

- safeguarding and empowering people, particularly the most vulnerable
    - a particular focus on: Children’s privacy, AI-driven discrimination, Direct marketing and DSARs
- taking enforcement action "where necessary to make a real difference in people's lives”
    - over the next 2 years, the ICO will trial a revised approach for the public sector – more warnings, more reprimands, more enforcement notices, fines in only serious cases
- promote openness and transparency
    - **NB:** names of any organisation with reprimands are now published on ICO website
    - **NB:** names of any organisation notifying a data breach or cyber incident are now published on ICO website
    - means an increased risk to reputational damage

What's the ICO interested in? Enforcement

Data Protection Fines – Why They Happen and How to Avoid Them

- Being irresponsible with people's data
  - Usually not taking adequate security measures to prevent or contain a serious personal data breach
- Seeing data protection as a one-time exercise
  - Systems, people and ways of working change all the time. It's your duty to assess and manage the risks you face on an ongoing basis
- Getting caught out by PECR
  - if you want to use any sort of electronic communications methods like email, telephone, or text messages to tell people about your products, services, ideas, or to raise funds, Privacy and Electronic Communications Regulations (PECR) must be considered as well as data protection
- Waiting until something goes wrong before taking action
  - If something does go wrong, any sensible steps taken to mitigate risks to people's personal data will be taken into account

What's the ICO interested in? Facial Recognition Tech

- North Ayrshire Council (NAC) considered using Facial Recognition Technology (FRT) to verify pupils' identities at the cash register during lunch, making it "cashless catering"

- Involved processing pupil special category data i.e. biometric data.

- Concerns were raised and this led to an enquiry by the ICO into the processing. The letter published by the ICO provides some useful guidance and lessons to learn from:

1. **Consent: you need a valid lawful basis**

    - Biometric data is special category data which requires both an Article 6 and Article 9 lawful basis under UK GDPR.
    - 'Consent' and 'Explicit Consent' are likely to be the most appropriate for things like cashless payment but consider other grounds for other use types
    - Consent must be "freely given" which means that pupils must be able to say 'no' without detriment and you must provide an alternative system (e.g. access to the same catering options using a physical cash register)

What's the ICO interested in? Facial Recognition Tech

2. Transparency: The use of FRT must be explained in a child friendly way

- Be clear what the data will be used for, if it will be shared, and the risks involved (e.g. any bias and discrimination)

3.Contracts: If you are using a 3rd party provider for FRT a compliant contract needs to be in place

- If the provider is a processor (which is likely) an Article 28 compliant contract in place
- If the data is exported then export rules need to be complied with
- The UK's International Data Transfer Agreement (IDTA) may be needed together with a Transfer Risk Assessment (TRA)

3. DPIA: You must complete one where biometric data is involved

- Processing children's biometric data via FRT will require a DPIA
- Ensure that risks of bias and discrimination in the use of FRT are identified, assessed and mitigated

What fines have we seen?

Entity	Breach	Country	Fine/Action Taken
BT Ltd	Sent 4.9 million emails related to charitable causes relying on “soft opt-in” instead of consent	UK	£77,000 [PECR]
Halfords Limited	Sent 500,000 marketing emails on basis of legitimate interests instead of consent	UK	£30,000 [PECR]
Tuckers Solicitors	Data breach (ransomware attack)	UK	£98,000
Dutch Tax and Customs Administration	Illegal processing of personal data	Netherlands	€3.7 million
Clearview AI Inc	Failing to have a lawful reason for collecting UK citizens data on facial recognition database	UK	£7.5 million
Bocconi University	Inappropriate use of remote monitoring software in online examinations	Italy	€200,000
Belgian School Board	Unlawful processing of personal data for under 13 year olds (no parental consent)	Belgium	€2,000
Headteacher of Isleworth Town Primary School	Illegal processing of sensitive personal data belonging to school children	UK	£1,099

Reforming Data Protection Laws in the UK

England Rugby

Official Legal Partner

irwinmitchell

Data Reform Bill

- The Data Protection and Digital Information (No. 2) Bill will be introduced to Parliament for a second reading today
- It was initially introduced in July 2022 but was withdrawn by Liz Truss' Government
- It is positioned as a "new common-sense-led UK version of the EU's GDPR" and wants to preserve adequacy
- Key issues include:
    - Clarifying what uses of data fall within 'legitimate interests'
    - Clarifying when you can process personal data without consent
    - Extend ability to use the soft opt-in to charitable, political or other non-commercial objectives, if the individual's contact details were obtained in the course of the individual expressing interest or offering support to the objective
    - Removing the need for a DPO and DPIA (but replacing them with something similar)
    - Replacing the "manifestly unfounded or excessive" threshold for refusing data subject rights requests with a "vexatious or excessive" threshold
    - Only businesses conducting activities that are likely to pose high risks to individual's rights and freedoms will be required to keep a record of processing activities

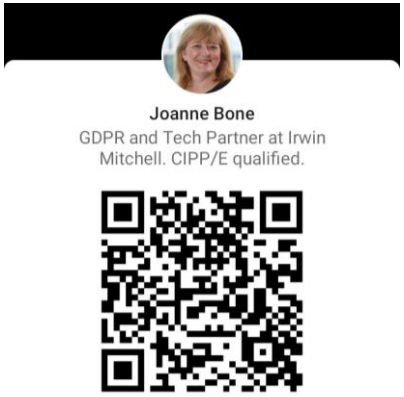
Q&A

England Rugby

Official Legal Partner

irwinmitchell

Your Speakers



Joanne Bone
Partner
Joanne.bone@irwinmitchell.com

Hannah Moran
Solicitor
Hannah.moran@irwinmitchel.com

England Rugby
Official Legal Partner

IM irwinmitchell

Expert Hand. **Human Touch.**