GDPR in schools and academies

Dai Durbridge, Partner

Browne Jacobson LLP

brownejacobson
education advisors

Welcome

- Partner in the Education team at Browne Jacobson
- Lead the Manchester Education team
- Expert information management lawyers

BROWNE JACOBSON LLP

Commitment to education

- National law firm with highly regarded education practice across our five offices, including Manchester
- Act for over 1,300 schools academies and colleges

Freedom and Autonomy for Schools - National Association
FASNA
Approved Partner

nga National Governors' Association
Approved partner

ISBL
Institute of School Business Leadership
Approved Partner

Premier partner
ASCL Association of School and College Leaders

Lexcel Practice Management Standard Law Society Accredited
INVESTORS IN PEOPLE

brownejacobson
education advisors

Why all the fuss about GDPR?

Very different data landscape than in 1998

Data data data data data

90% of all the **data** in the world today has been created in the past few years

2.5 exabytes - that's 2.5 billion gigabytes (GB) - of **data** was **generated** every day in 2012

Data per minute today

- 216,000 Instagram posts
- 204,000,000 emails
- 12 hours of footage is uploaded to YouTube
- 277,000 tweets are posted

Key points

- Comes into effect on 25 May 2018 across Europe
- Data Protection Bill issued to implement GDPR in UK
- Main concepts and principles remain the same, but new elements of it enhance the provisions under the DPA
- Some hefty fines…

Enforcement

- Elizabeth Denham, the Information Commissioner (ICO)

- Up to €20,000,000 fine

The core concepts

GDPR concepts

1. Data protection principles
2. Individuals' rights
3. Accountability

1. Data protection principles – Article 5

Personal data must be:

- lawfully, fairly and transparently processed
  - Fair processing or privacy notice
  - Being clear

- processed for a specific, explicit and legitimate purpose
  - Why are you processing?
  - What is the purpose?

1. Data protection principles – Article 5

Personal data must be:

- Adequate, relevant and limited to what is necessary in relation to the purpose(s)
  - Data minimisation – only keep what you need
- Accurate and, where necessary, kept up to date
  - Reasonable steps should be taken
- Only kept for as long as is necessary for the purpose

2. Individuals' rights

1. Right to information (Article 13)
   - Fair processing notice
   - Data processing notices

2. Subject access rights
   - Free
   - One month to comply

3. Accountability

DPO

Data breach notification

Privacy by design

Records of processing

Impact assessment

Controllers and processors

Demonstrate compliance and accountability

- You will need to be able to show compliance in:
  - Requirement to implement appropriate technical and organisational measures
  - Maintaining records on processing activities
  - Data protection impact assessments
  - Requirement to appoint a DPO
  - Data protection by design
  - Codes of conduct and certification schemes

10 steps to take now

1. Awareness and leadership

- Make sure decision makers aware of change and impact
- Nominate a responsible member of SLT
- Organise a working group (IT, HR) and put regular meetings in the diary
- Add data protection to your risk register

2. Information you hold

- Document the information you hold
  - Where did it came from?
  - With whom do you share it?
  - Why are you keeping it?

- Carry out a data mapping exercise

3. Third party contracts

- Do you share information with other companies?
  - Payroll?
  - Catering contractors?

- Review the contracts. If they go beyond 25 May 2018 they will require amendment to reflect GDPR changes

4. Privacy notices and retention/destruction

- New privacy notices must include:
  - Legal basis for processing
  - Data retention periods
  - Complaints
  - Concise, easy to understand and language

- New DfE model now available

- What about retention and destruction policies?

5. Individual rights and subject access request

- Check procedures to make sure they cover all new rights
- No fee
- Must be provided in writing unless otherwise requested (requestor can ask for electronic format)
- Must respond within one month - can extend for complex requests

6. Consent

- Must be freely given, specific, informed and unambiguous, and a **positive affirmation** of the individual's agreement
- As the consent must be freely given it cannot be bundled in with other consents
- Withdrawal of consent should be as easy as grant of consent

Review how you seek, obtain and record consent and whether you need to make changes

Burden on school to show consent freely given

7. Data breach management

- Must have procedures in place to detect, report and investigate a personal data breach
- 72 hours from the discovery of the breach to report to ICO
- Breach must be reported unless the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons
- Notify the affected data subjects

Appoint your DPO

- Responsible for monitoring GDPR compliance and implementation/application of data protection policies
- DPO must have expert knowledge of data protection law and practice
- No need to appoint a new person or outsource
- What about positions of conflict?

9. Staff practices

…(Governors and trustees/directors too)

- Use of personal emails rather than trust emails?
- Taking hard copy personal data home/out of school?
- Downloading data onto a non-school device?
- USBs, discs, data rooms etc.

Action - Use this opportunity to review and improve

10. Training/re-education

- Train staff to recognise a subject access request
- Train/re-educate regarding data security and off site use
- If policies are changed, consider how you disseminate and evidence staff understanding
- What other training might they need?

Question?

Please note

The information contained in these notes is based on the position at January 2018. It does, of course, only represent a summary of the subject matter covered and is not intended to be a substitute for detailed advice. If you would like to discuss any of the matters covered in further detail, our team would be happy to do so.

Dai Durbridge | 0330 045 2105 |
dai.durbridge@brownejacobson.com

GDPR in schools and academies

Dai Durbridge, Partner

Browne Jacobson LLP

brownejacobson
education advisors