

DPO Foundation Training

Dai Durbridge and Daljit Kaur

Browne Jacobson LLP

Our objectives...

...are that you:

1. understand and can adequately discharge your DPO role
2. leave feeling confident that you know all you need to
3. enjoy the day and have all your questions answered

Today

What are your objectives?

Status update!

Data audit?

Policies, procedures and documents updated?

DPO appointed...?

...and after today, DPO suitably trained

25 May 2018

- The world will not end
- It is not a deadline - it's a start line
- Don't worry about it

The plan for today

- Some sludgy stuff to get through
- ...then plenty of workshops, case studies, and other hands on learning

- Practical
- Commercial
- Helpful
- Clear and simple

Let's get started

Final points:

- DPO -v- DSL
- DPO support after today

Please note

The information contained in these notes is based on the position at May 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.

© Browne Jacobson LLP 2018. Browne Jacobson LLP is a limited liability partnership.



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

Please note

The information contained in these notes is based on the position at May 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.

© Browne Jacobson LLP 2018. Browne Jacobson LLP is a limited liability partnership.



Daljit Kaur | 0330 045 2281
daljit.kaur@brownejacobson.com

The role of the DPO

review of the role, what the law require of DPOs and understanding how to discharge the duty in your school

Dai Durbridge

Browne Jacobson LLP

Role of the DPO

- How are you feeling about your role?
- What are your fears?
- How much work do you think the role will be?

Role of the DPO

- On average, about 2-3 hours per week
- More if there is a data breach to manage
- Sound right to you?
- What will that time be spent doing?

Understanding the role

Articles 37-39

- Monitor GDPR compliance and implementation and application of data protection policies
- Inform/advise school and staff about GDPR obligations
- Inform/advise processors engaged with the school
- Carry out internal data audits

Understanding the role

Articles 37-39 (cont.)

- Be the point of contact for the ICO
- Train staff
- Manages breaches
- Advise whether and how to carry out DPIA

Data Protection Impact Assessments

DPO should be able to advise on the following in respect to the DPIA:

- whether to carry out a DPIA
- what methodology to follow when carrying out a DPIA
- whether to do it in-house or outsource it

Data Protection Impact Assessments

Data Protection Impact Assessments

DPO should be able to advise on the following in respect to the Data Protection Impact Assessments (cont.):

- safeguards to apply to mitigate risks to data subjects
- whether the DPIA has been correctly carried out and whether its conclusions comply with the GDPR

Data Protection Impact Assessments

ICO process diagram:



Data Protection Impact Assessments

- Not likely to be a regular occurrence
- Should not be particularly onerous to complete
- Have a template ready

Understanding the role

DPO involvement - You must ensure that:

- The DPO is involved in all issues relating to the protection of personal data
- The DPO reports to your highest management level - i.e. school governors/MAT Board
- The DPO operates independently and is not dismissed or penalised for performing their task

Understanding the role

DPO involvement - You must ensure that (cont.):

- Adequate resources are provided to enable DPOs to meet their GDPR obligations
- The DPO can be contacted by data subject on all issues relating to the processing of their personal data

Understanding the role

Importantly...

DPO's will not be personally responsible for non-compliance with the GDPR as this is the responsibility of the Controller or Processor

Skills and support required

Qualifications

No precise credentials specified by the GDPR, but....

- DPO must have expert knowledge of data protection law and practice - **proportionate to the type of processing the school carries out**

Skills and support required

Art 29 Working Party - necessary skills & expertise include:

- expertise in national and European data protection laws and practices including an in-depth understanding of the GDPR
- understanding of processing operations carried out
- understanding of information technologies and data security
- knowledge of the business sector and the organisation
- able to promote data protection culture within organisation

Skills and support required

Support by your school/trust

- Active support of the DPO function by senior management
- Sufficient time and resources for DPO to fulfil their duties
- Communicate designation of DPO to all staff
- Continuous training

Skills and support required

Support by your school/trust (cont.)

- Do you foresee any challenges with support from your school?
- How are you going to overcome them?

*

Peer to peer support

- How could your experiences help each other?
- What could you share?
- Is there merit in creating local groups to share information, experiences and learning?
- What else could you do?

*

Understanding the role

- Discuss as an SLT
- Compare to DSL role
- Discuss with them current practices at the school, the risks those practices pose and the likely consequences of breach
- We will arm you with those details by the end of today

*

Summary

- Brand new role - it'll take time to get used to it
- Not as scary or as onerous as some have made it out to be
- Think about how you will work with the SLT to ensure you have the right support
- Start thinking now about peer to peer support

The role of the DPO

review of the role, what the law require of DPOs and understanding how to discharge the duty in your school

Dai Durbridge

Browne Jacobson LLP

Understanding the law

an overview of the key data protection laws and how to interpret them and comply with them

Daljit Kaur

Browne Jacobson LLP

Relevant Legislation

Four pieces to know about:

1. General Data Protection Regulation 2016
2. The Data Protection Bill
3. Privacy and Electronic Communications Regulations (PECR)
4. Data Protection (Charges and Information) Regulations 2018

1. General Data Protection Regs 2016 (GDPR)

GDPR

- The most comprehensive of the four bits of law
- It includes:
 - Data protection principles
 - Processing personal data
 - Rights of data subjects
 - Responsibilities of data controllers and data processors
 - ICO powers
 - Transfer to third countries

GDPR

- Comes into effect on 25 May 2018
- Main concepts and principles remain the same, but new elements of it enhance the provisions under the current DPA
- Requires a regulatory body - ICO - to monitor and ensure compliance

Purpose of GDPR

- To harmonise protection of fundamental rights and freedoms of natural persons in respect of processing activities
- To ensure free flow of personal data between Member States

Accounting for technological changes and increase in data use

Application of GDPR

- Any information concerning identified or identifiable natural living persons
- Processing of personal data:
 - wholly or partly by automated means; and
 - other than by automated means of personal data which forms part of a filing system or are intended to form part of a filing system (Article 2)

Key provisions

- 171 Recitals providing detail
- 99 Articles setting out provision and derogations
- Definitions are covered in Article 4, e.g.
 - Personal Data
 - Processing
 - Filing System
 - Controller
 - Processor
 - Consent
 - Personal Data Breach
 - Supervisory authority

New Data Protection Principles

The GDPR requires:

- (a) Data to be processed lawfully, fairly and in a *transparent* manner
- (b) Data to be collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes
- (c) Processing of data should be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed

New Data Protection Principles - Article 5

The GDPR requires (cont.):

- (d) Data to be accurate and, where necessary, kept up to date - inaccurate data should be erased or rectified without delay
- (e) Data to be kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed

New Data Protection Principles - Article 5

The GDPR requires (cont.):

- (f) Data to 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.

The data controller must be able to demonstrate compliance with these principles as well as accountability.

New Data Protection Principles - Article 5

- Data Protection Principles underpin GDPR
- All our processing must fit within them
- A good starting point when deciding whether what we want to do with data is legal
- Now we need to understand about processing personal data and processing special categories of personal data...

Processing personal data

For personal data to be processed lawfully you must satisfy one of the processing conditions:

- 6(1)(a) - consent of the data subject
- 6(1)(b) - processing is necessary for the performance of a contract with the data subject or to enter into a contract
- 6(1)(c) - processing is necessary to comply with a legal obligation

Processing personal data

For personal data to be processed lawfully you must satisfy one of the processing conditions (cont.):

- 6(1)(d) - processing is necessary to protect the vital interests of a data subject or another person
- 6(1)(e) - processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller
- 6(1)(f) - necessary for the purposes of legitimate interests

Processing special categories of personal data

For special categories of data to be processed lawfully you must be able to satisfy one of the following conditions:

- 9(2)(a) - consent of the data subject
- 9(2)(b) - processing is necessary for carrying out obligations under employment, social security or social protection law, or a collective agreement
- 9(2)(c) - processing is necessary to protect vital interests of data subject or another individual

Processing special categories of personal data

For special categories of data to be processed lawfully you must be able to satisfy one of the following conditions (cont.):

- 9(2)(d) - processing carried out by a not-for-profit body with a political, philosophical, religious or trade union aim.....
- 9(2)(e) - processing relates to personal data manifestly made public by the data subject
- 9(2)(f) - processing is necessary for establishment, exercise or defence of legal claims

Processing special categories of personal data

For special categories of data to be processed lawfully you must be able to satisfy one of the following conditions (cont.):

- 9(2)(g) - processing necessary for substantial public interest on basis of EU or English law which is proportionate to aim pursued and which contains appropriate safeguards
- 9(2)(h) - processing necessary for purpose of preventative or occupational medicine, assessing working capacity of employee, diagnosis, provision of health/social care or treatment or management of health or social care systems

Processing special categories of personal data

For special categories of data to be processed lawfully you must be able to satisfy one of the following conditions (cont.):

- 9(2)(i) - relates to public interest in the area of public health
- 9(2)(j) - processing is necessary for archiving purposes in the public interest, or scientific and historical research purposes or statistical purposes in accordance with Article 89(1)

Processing

- Processing has a broad definition and includes collecting storing, using and sharing data
- As well as setting out in law what we can do with personal data and special categories of personal data, GDPR also sets out the rights of the data subjects

Rights of data subjects

GDPR protects the data subjects and provides them with rights to ensure they can exercise greater control over their data.

These rights are:

1. Right to information
2. Subject access rights
3. Right to rectification

Rights of data subjects

4. Right to erasure (right to be forgotten)
5. Right to restrict processing
6. Right to data portability
7. Right to object
8. Rights in relation to automated decision making and profiling

Remedial rights of data subjects

- Complaint to ICO
- Judicial remedy against the controller, processor or ICO
- Compensation for damage suffered as a result of infringement

Data controllers and data processors

What's the difference?

- **Data controller** - a person who (either alone or jointly or in common with other persons) determines the purposes for which and the manner in which any personal data are, or are to be processed
- **Data processor** - means any person (other than an employee of the data controller) who processes the personal data on behalf of the data controller

Responsibilities as Data Controller

- Implement appropriate technical/organisational measures to ensure and demonstrate GDPR compliance
- Implement appropriate policies
- Only use processors guaranteeing to implement appropriate technical/organisational measures to ensure compliance
- Co-operate with ICO
- Data Protection by design and by default

Responsibilities as Data Processor

- Will not engage another processor without prior written authorisation from the controller
- Processing governed by written contract or other legal act setting out subject matter/duration of processing, nature and purpose, types of personal data and categories of data subjects and obligations and rights of controller
- Personal data processed only on controller instructions
- Co-operate with ICO

Processing of Data

- Each controller to maintain a record of processing activities under its responsibility
- Each processor to maintain a record of categories of processing activities carried out on behalf of the controller
- The ICO as supervisory body can request copies of these records
- Our advice...

Technical and organisation measures

Data security - such as:

- Pseudonymisation and encryption of personal data
- Ensuring ongoing confidentiality, integrity, availability and resilience of processing systems and services
- Ability to restore availability and access to personal data in a timely manner in the event of physical or technical accident
- Regular testing, assessing and evaluating the effectiveness of security measures

Data breaches

- Governed by GDPR
- More on this later...

ICO powers - investigative

- Order a controller/processor to provide information
- Carry out investigations - data protection audits
- Notify controller/processor of any alleged infringements
- Access all personal data from controller/processor
- Access any premises and processing equipment of controller/processor

ICO powers - corrective

- Issue warnings to controller/processor if intended processing operations likely to infringe GDPR
- Issue reprimands where processing has infringed GDPR
- Order processing operations are brought into compliance
- Order controller to communicate breach to data subject
- Limit or ban processing temporarily or indefinitely
- Order rectification or erasure
- Impose a fine or withdraw certification

Transfer to third countries etc.

- Can take place where EU has decided that the third country or international organisation or territory or sector therein ensures adequate level of protection
- Where no EU decision, personal data can be transferred to a third country or international organisation only if the controller or processor has provided appropriate safeguards, and data subjects can enforce their rights and legal remedies

2. Privacy and Electronic Comms Regs 2003

PECR 2003

- Known as “e-privacy Directive” it complements general data protection regime and sets out more specific privacy rights on electronic communications
- EU in the process of replacing PECR with a new e-privacy regs to sit alongside the GDPR - not yet agreed
- For now, PECR still applies

PECR covers

- Marketing by electronic means - calls, texts, emails, faxes
- Use of cookies etc. to track websites access information
- Security of public electronic communications services
- Privacy of customers using communications networks

PECR applies to

- Those who provide public electronic communications network or service and also those that:
 - market by phone, email, text or fax
 - use cookies etc. on their website

PECR and GDPR

- Current form of PECR still applies
- Where consent required for the purposes of PECR, it will be the standard of consent under GDPR
- Sending electronic marketing and using cookies etc. will require compliance with both PECR and GDPR
- The ICO will monitor compliance where PECR is also relevant

3. Data Protection Bill 2018

Data Protection Bill 2018

- Approaching final stages - currently 206 Sections and 18 Schedules
- Includes provision for derogations permitted by the EU
- Permits Secretary of State to introduce Regs, for example for fees which controllers can charge
- Sets role of the Information Commissioner

4. Data Protection (Charges and Information) Regs 2018

Data Protection (C&I) Regs 2018

- Sets out:
 - charges payable to the Information Commissioner
 - requirement for data controller to provide Information Commissioner with specified details
 - the requirements on Governing Bodies and Headteacher can be met with details of the school

Summary

- GDPR is the main piece of legislation and your go to place for detail
- Governs 95% of your processing
- PECR to be updated, but remains law for the moment
- New Data Protection Act 2018 imminent...

Understanding the law

an overview of the key data protection laws and how to interpret them and comply with them

Daljit Kaur

Browne Jacobson LLP


The five lawful bases for processing data in schools

understanding which basis to rely on and ensuring consent if fairly, lawfully and transparently obtained

Daljit Kaur

Browne Jacobson LLP

The five lawful bases

- 
1. Consent
 2. Contract
 3. Legal obligation
 4. Vital interests
 5. Public task

1. Consent

- The lawful basis of last resort
- The weakest basis
- Why...?

1. Consent

Data subject has consented to processing of personal data for one or more specific purposes

- Ideally this should be last ground you rely on because:
 - Consent can be easily withdrawn
 - Issues concerning full engagement with everyone
 - If used in addition to another ground, withdrawal of consent may prevent processing you would otherwise be permitted to undertake

1. 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

Burden on school to show consent freely given

1. Consent

- Consent not to be used where there is clear imbalance between data subject and the controller
- Consent is not freely given where data subject
 - has not been able give separate consent to different personal data processing
 - the performance of a service is dependent on the consent despite such consent not being necessary for such performance

1. Consent

- Do you need to renew existing consents?
- No, as long as...
 - processing is based on consent pursuant to previous 95 EU directive, consent is not required where the manner in which the consent was given was in line with the conditions of the GDPR

1. Consent of children and ISS

- ISS - Information Society Services. Which means...?
- Only applicable to ISS offered to children directly
- Consent of children over the age of 13 (Data Protection Bill), otherwise consent of the parent required

1. Consent - summary

- Shift in approach - more power given to the individual
- Consent may well be withdrawn by pupils and parents
- How will you manage it?

2. Contract

Processing is necessary for performance of a contract to which data subject is party or in order to take steps at request of data subject prior to entering into a contract

Condition:

- It is **necessary** to process the personal data:
 - to fulfil contractual obligations to data subject; or
 - data subject has asked you to do something before entering into a contract

2. Contract

When will processing be “**necessary**” for this ground?

- Necessary - in terms of being a proportionate way of achieving the purpose
- If there are other less intrusive ways to meet the contractual obligations this ground cannot be relied on
- Consider other contractual requirements, especially around the age of a child etc.

3. Legal Obligation

Processing is necessary for compliance with a legal obligation to which controller is subject

- For processing to comply with a legal obligation
- Must be **necessary** to process the personal data to fulfil the legal obligation
- If the obligations can be complied with in another way, this legal basis will not apply
- ICO states you should be able to either identify specific legal provision or an appropriate source of advice re obligation

4. Protecting Vital Interests

Processing is necessary in order to protect vital interests of the subject or of another natural person

- Vital interest - to protect an interest which is essential for life of the data subject or that of another natural person
- Another natural person - should only take place where the processing cannot be manifestly based on another legal basis
- Where emergency medical treatment is required - but consider requirements for processing Special Category data

5. Task carried out in the public interest

Processing is necessary for performance of a task carried out in public interest or in the exercise of official authority vested in the controller

- Task or official authority should be set out in law (i.e. have a clear legal basis but not necessarily a legislative act - so includes case law and statutory guidance etc.)
- If the obligations can be complied with in another less intrusive way, this legal basis will not apply

Special Categories of personal data: Additional requirements for lawful processing for schools

Processing Special Categories of Personal Data

Article 9(1)

Processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation shall be prohibited

Unless any of the grounds in 9(2) also apply

Lawful processing of special category data

- Is it just personal data or Special Category Data?
- Is the processing necessary or can the goal be achieved without processing personal data?
- Which of the five lawful bases is most appropriate?
- If Special Category data then you need a general processing bases for personal data but also an additional ground for processing Special Category of data

Lawful processing of special category data

Scenarios where you may be processing Special Category Data include:

- Informing staff that special arrangements need to be made for a child with SEN e.g. sharing an IEP or EHCP
- Informing the HR department the reason for a staff member requiring time off work for health reasons

Summary

- Do you actually need to process personal data? If there is an alternative, explore that first
- If processing personal data, is it is Special Category Personal Data? If so, is an additional ground for processing required?
- If processing personal data only, consider basis for processing
 - Legal Obligation/Contract/Vital Interests/Public Task
- If none of the above, consider Consent as **LAST RESORT**

The five lawful bases for processing data in schools

understanding which basis to rely on and ensuring consent if fairly, lawfully and transparently obtained

Daljit Kaur

Browne Jacobson LLP

Ensuring and monitoring compliance

the practical steps to take to discharge your duty and ensuring you can evidence compliance

Dai Durbridge

Browne Jacobson LLP

Monitoring compliance

Two parts:

- Policies, procedures and documents
- Actions

Policies, procedures and documents

- Get them in place
- Reputable source
- Approved by governors as appropriate

Policies, procedures and documents

- Need to evidence:
 - Creation
 - Sharing
 - implementation

- How will you do it?

*

Monitoring compliance

- How do you evidence that staff *actions* are compliant with your policies and procedures?

Internal audits

What would your audit look like and how often would you do it?

*

Internal audits

Review:

- SAR requests and completed disclosures
- retention and destruction of documents
- information sharing - LAs, third party processors
- pupil consents to ensure they are followed

What else?

*

Internal audits

- How often?
- What evidence would you create to show you carried out an audit?

**

Internal audits

Top tip:

- What does your DSL do...?
- If it works for them, it's likely to work for you
- No need to reinvent the wheel...

Monitoring compliance

- Monitoring is a little bit pointless if you cannot evidence it...
- Focus on evidencing outcomes, not inputs
- How can you evidence staff understanding and compliance?
 - Staff meetings?
 - Stop and question staff?
 - But what evidence of compliance has been created?

Monitoring compliance

- Evidence based monitoring:
 - Staff quiz
 - Survey
 - Staff training methods (more later)

- What would you include in a staff quiz?

**

Monitoring compliance

Top tip:

- Keep the questions relevant, short and on the easy side
- Require short answers - easier to complete and easier for you to check and analyse
- Hammer home key points by having the same answer to a few of the questions

Monitoring compliance

- What evidence do they provide?
- How do you assess that evidence?
- What actions does that evidence suggest are necessary?

**

Summary

- Key part of your DPO role
- Focus on evidencing outcomes
- Creates evidence for improvement and, importantly, to defend a breach (more later)
- Learn from the DSL approach

Ensuring and monitoring compliance

the practical steps to take to discharge your duty and ensuring you can evidence compliance

Dai Durbridge

Browne Jacobson LLP

Training and updating

Keeping yourself and your staff trained and updated and how best to measure and evidence outcomes

Dai Durbridge

Browne Jacobson LLP

Training and updating

What does your DSL do...?

Training and updating

- DSL has the same duty as set out in Keeping Children Safe in Education guidance
- Don't reinvent the wheel...
- Easier for your staff to engage because they are used to that approach

Training and updating

- Two groups:
 - You
 - Your staff

- Two types:
 - Initial training and upskilling
 - Ongoing updates

Training and updating

Four points to consider for all training and updates:

1. What's available?
2. What's reliable and digestible?
3. What format is the best?
4. How can you evidence the outcomes?

1. What's available?

- Anything and everything if you've got time to look for it!
- All formats, all qualities, all styles, all lengths, all school types - you can generally find something on the web
- That doesn't mean it's worth finding...
- Focus on the questions two and three

2. What's reliable and digestible?

- Reliable
 - Where did you get it from?
 - Who produced it?
 - When was it produced?
- Digestible
 - If it's not, it's not useful
 - What format works best for your staff - ask them
 - Lite bites often best - but ask your staff

3. What format is best?

- Not about *ease* of training or updating, but the extent to which it is absorbed
- What works best for them?
 - Writing - Articles, Emails webpages
 - Visual - Webinars, recordings, online presentations
 - In person - staff meetings, lite bite sessions
 - Larger scale - conferences, workshops
- Topics may dictate the best format

**

4. How do you evidence the outcomes?

Important for proving compliance with guidance and satisfying yourself that staff are appropriately updated

- Sign in sheets
- Copies of emails, articles, presentations
- What else?

- How can you evidence staff engagement as opposed to receipt?

4. How do you evidence the outcomes?

What did you decide when we talked about evidencing culture change?

And remember...

Training and updating

- What evidence do they provide?
- How do you assess that evidence?
- What actions does that evidence suggest are necessary?

Summary

- Key part of your DPO role
- Focus on evidencing outcomes
- Creates evidence for improvement and, importantly, to defend a breach (more later)
- Learn from the DSL approach

Training and updating

Keeping yourself and your staff trained and updated and how best to measure and evidence outcomes

Dai Durbridge

Browne Jacobson LLP

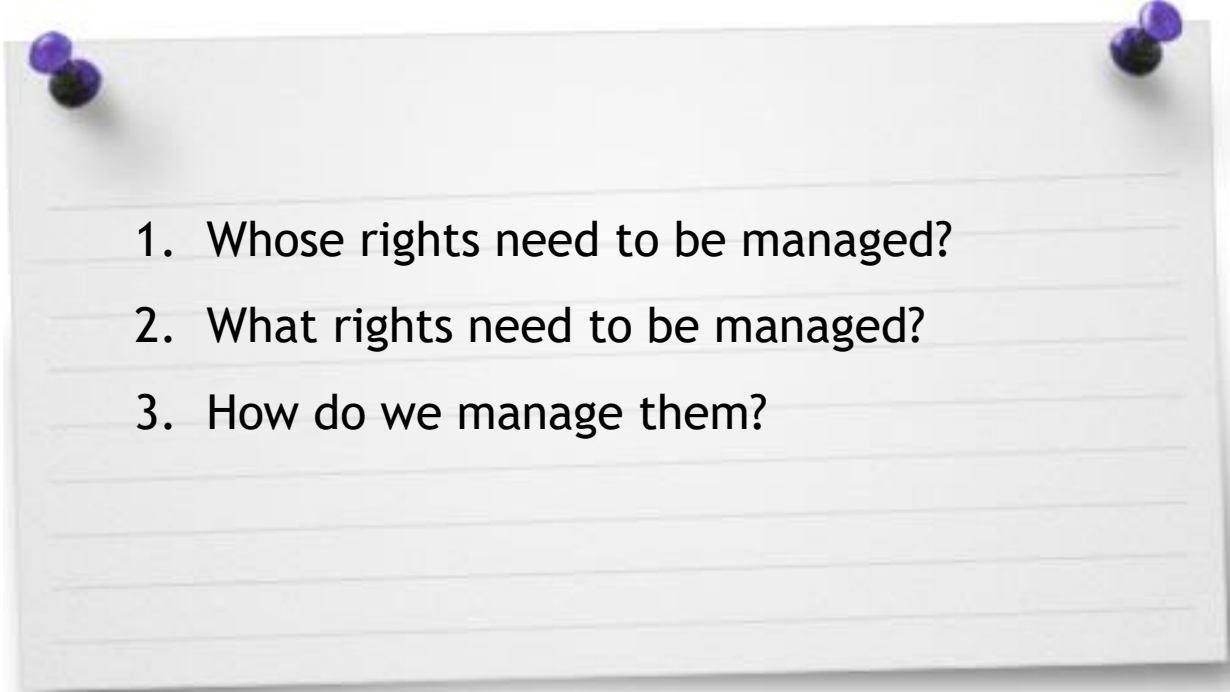
Managing individual rights

understanding the rights individuals have, handling subject access requests and how to deal with requests for erasure and for inaccuracies to be corrected

Daljit Kaur

Browne Jacobson LLP

Three key issues

- 
1. Whose rights need to be managed?
 2. What rights need to be managed?
 3. How do we manage them?

1. Whose rights need to be managed?

Categories of data subjects

- Students
- Parents/carers
- Additional contacts e.g. baby sitters/after school

- Workforce:
 - Staff
 - Volunteers
 - Governors
 - Trustees/Members
 - Contractors

2. What rights need to be managed?

Rights of data subjects

We covered this earlier.... These rights are:

1. Right to information
2. Subject access rights
3. Right to rectification

Rights of data subjects

4. Right to erasure (right to be forgotten)
5. Right to restrict processing
6. Right to data portability
7. Right to object
8. Rights in relation to automated decision making and profiling

1. Right to information (art 13 and 14)

At the time information is collected from the individual you need to provide the following:

- (a) identity and the contact details of the controller
- (b) DPO contact details
- (c) purposes and legal basis for processing personal data
- (d) the recipients/categories of recipients of the personal data

1. Right to information (art 13 and 14)

At the time information is collected from the individual you need to provide the following (cont.):

- (e) if applicable, fact that controller intends to transfer personal data to third country and existence/absence of an adequacy decision by the Commission, or where required reference to appropriate or suitable safeguards and means by which to obtain a copy of them or where they have been made available

This shall not apply where and insofar as the data subject already has the information

1. Right to information (art 13 and 14)

At the time information is collected the individual should also be informed of:

- (a) period for which the personal data will be stored, or if not possible, criteria used to determine that period
- (b) details of their right to request access to, rectification of or erasure of personal data or restriction of processing concerning the data subject or to object to processing as well as the right to data portability

1. Right to information (art 13 and 14)

At the time information is collected the individual should also be informed of:

- (a) period for which the personal data will be stored, or if not possible, criteria used to determine that period
- (b) details of their right to request **access** to, **rectification** of or **erasure** of personal data or **restriction** of processing concerning the data subject or to **object** to processing as well as the right to data **portability**

1. Right to information (art 13 and 14)

At the time information is collected the individual should also be informed of (cont.):

- (c) where processing is as a result of consent the existence of the right to withdraw consent at any time
- (d) right to lodge a complaint with the ICO
- (e) whether provision of personal data is statutory/contractual requirement, or requirement necessary to enter a contract, as well as whether data subject is obliged to provide the personal data and possible consequences of failure to do so

1. Right to information (art 13 and 14)

At the time information is collected the individual should also be informed of (cont.):

- (f) existence of automated decision-making, including profiling and, at least in those cases, meaningful information about logic involved, as well as significance and envisaged consequences of such processing for data subject

This shall not apply where and insofar as data subject already has the information

1. Right to information (art 13 and 14)

When information is **not** obtained from data subject, he/she must be provided with the following:

- (a) identity and contact details of controller
- (b) DPO contact details
- (c) purposes and legal basis for processing personal data
- (d) categories of personal data concerned

1. Right to information (art 13 and 14)

When information is **not** obtained from data subject, he/she must be provided with the following (cont.):

- (e) recipients or categories of recipients of the personal data, where applicable
- (f) if applicable, fact that controller intends to transfer personal data to third country and existence/absence of an adequacy decision by the Commission, or where required reference to appropriate or suitable safeguards and means by which to obtain a copy of them or where they have been made available

1. Right to information (art 13 and 14)

When information is **not** obtained from data subject, he/she should be provided with the following (cont.):

- (a) period for which personal data will be stored, or if that is not possible, the criteria used to determine that period
- (b) details of their right to request access to, rectification of or erasure of personal data or restriction of processing concerning the data subject or to object to processing as well as the right to data portability

1. Right to information (art 13 and 14)

When information is **not** obtained from data subject, he/she should be provided with the following (cont.):

- (c) where processing is based on consent, existence of right to withdraw consent at any time
- (d) right to lodge a complaint with the ICO
- (e) from which source data originated, and if applicable, whether it came from publicly accessible sources

1. Right to information (art 13 and 14)

When information is **not** obtained from the data subject, he/she should be provided with the following (cont.):

- (f) existence of automated decision-making, including profiling, and, at least in those cases, meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject

Within a reasonable time but at least within 1 month

2. Subject Access Requests (art 15)

What can it cover?

- right to obtain from controller confirmation as to whether or not personal data concerning him/ are being processed
- access to the personal data being processed
- purposes of the processing
- categories of personal data concerned

2. Subject Access Requests (art 15)

What can it cover (cont.)?

- recipients/categories of recipient to whom personal data have been or will be disclosed, in particular recipients in third countries or international organisations
- if possible, envisaged period for which personal data will be stored, or if not possible, criteria used to determine period
- details of rights to rectification/erasure/restriction or objection to processing

2. Subject Access Requests (art 15)

What can it cover (cont.)?

- right to complain
- source of information if not from the individual
- existence of automated decision making/profiling

3. Right to rectification (art 16)

- Can request that:
 - without undue delay controller rectifies any inaccurate data about the data subject
 - that incomplete personal data about the data subject be completed (dependent on the purpose of processing)
- **Question:** Is it really inaccurate or are they just unhappy about the information recorded?

4. Right to erasure (to be forgotten) (art 17)

Can request that without undue delay the controller erases the data it holds about the data subject, where:

- personal data no longer necessary in relation to the purposes for which they were collected or otherwise processed;
- processing was under consent and data subject withdraws consent and where no other legal ground for processing exists
- data subject objects to processing for public task, exercise of legitimate duty/interest and direct marketing and there are no overriding legitimate grounds for the processing

4. Right to erasure (to be forgotten) (art 17)

Can request that without undue delay the controller erases the data it holds about the data subject, where (cont.):

- personal data have been unlawfully processed
- personal data have to be erased for compliance with a legal obligation in EU or English law to which controller is subject
- personal data have been collected in relation to offer of information society services

4. Right to erasure (to be forgotten) (art 17)

- If you made personal data public and are required to erase it, taking account of available technology and cost of implementation, you need to take reasonable steps to inform other controllers about the request for erasure
- This request does not need to be complied with where processing is necessary for:
 - exercising right of freedom of expression and information
 - compliance with legal obligations/performing tasks carried out in public interest or in exercise of controller's official authority

4. Right to erasure (to be forgotten) (art 17)

- This request does not need to be complied with where processing is necessary for (cont.):
 - reasons of public interest in the area of public health
 - archiving purposes in the public interest, scientific, or historical research purposes or statistical purposes
 - establishment, exercise or defence of legal claims

5. Right to restrict processing (art 18)

- Can request controller restricts processing where:
 - accuracy of personal data is contested by data subject, for a period enabling the controller to verify the accuracy of the personal data
 - processing is unlawful and data subject opposes the erasure of personal data and requests restriction of their use instead
 - controller no longer needs personal data for purposes of processing, but are required by data subject for establishment, exercise or defence of legal claims

5. Right to restrict processing (art 18)

- Can request controller restricts processing where (cont.):
 - data subject has objected to processing for public interest task, exercise of legitimate duty/legitimate interest, pending the verification whether legitimate grounds of controller override those of data subject

If these apply, only limited processing can occur e.g. storage, or with consent or for establishing, exercising or defending legal claims; or protection of rights of another natural or legal person

6. Right to data portability (art 20)

- Individuals has right to receive personal data they provided to a controller in structured, commonly used and machine readable format
- They can also request that a controller transmits this data directly to another controller.
- Can only request this where:
 - processing is based on consent or on a contract pursuant; and
 - processing is carried out by automated means

7. Right to object (art 21)

- Individuals has right to object to processing undertaken for:
 - performance of task carried out in public interest or in exercise of official authority vested in the controller
 - purposes of legitimate interests pursued by controller or third party, except where such interests are overridden by interests or fundamental rights and freedoms of data subject which require protection of personal data, in particular where data subject is a child
- They can also object to direct marketing
- All the above includes objection to profiling

8. Automated decision making/profiling (art 22)

- Data subject has right not to be subject to decision based solely on automated processing, including profiling, which produces legal effects or significantly affects him or her
- Limited to situations where:
 1. processing not necessary for entering into/performing contract with data subject
 2. has not otherwise been authorised by law
 3. data subject did not provide explicit consent

If 1 or 3 applies, data controller should put measures in place to protect rights and freedoms e.g. by permitting the right to human intervention

3. How do we manage them?

Complying with requests

- Identify requestor and check personal data relates to them
- Provide information about action taken by controller without undue delay and at latest within month of receiving request
- Compliance period can be extended by further 2 months if complex or a number of requests
- If requested by electronic means, information should be provided by electronic means unless different format requested

Complying with requests

- No fee, but if requests are manifestly unfounded or excessive, you can either:
 - Charge a reasonable fee for admin costs; or
 - Refuse to act on the request

Onus is on you to demonstrate the request was manifestly unfounded or excessive

Complying with requests

- Where you have complied with request to rectify, erase or restrict processing you need to communicate this to anyone with whom you have shared personal data
- Exception is where this proves impossible or involves disproportionate effort
- You need to inform data subject about those recipients if requested

Managing individual rights

understanding the rights individuals have, handling subject access requests and how to deal with requests for erasure and for inaccuracies to be corrected

Daljit Kaur

Browne Jacobson LLP

Effectively managing a data breach

ensure breaches are known, managed and remedied immediately, when to advise the ICO and reporting the right information quickly to reduce any potential fine

Dai Durbridge

Browne Jacobson LLP

Tis important stuff...

Remember - fines of up to €20,000,000

Tis important stuff...

Effective management can save you £100,000+

Tis important stuff...

Really effective management could even
reduce the fine to zero...

Managing a data breach

- Must have procedures in place to detect, report and investigate a personal data breach
- Does your procedure do that?

Tis important stuff...

- South East Local Authority
- Police Force
- Local Authority (some years ago)

Managing a data breach

- Breach must be reported unless breach is unlikely to result in a risk to the rights and freedoms of natural persons
- 72 hours from the discovery of the breach to report to ICO
- May have to notify the affected data subjects

Managing a data breach

- 72 hours is not a long time
- If you have a data breach right now, when does your 72 hours end?
- If you have a data breach at 4pm on Thursday, when is your time up?
- Use them effectively by planning now

Managing a data breach

A staff member downloads pupil safeguarding information onto a memory stick and loses it but doesn't tell you

The first you hear about it is when the parent concerned tells you people have been talking about her child's safeguarding history on Facebook for the last 10 days or so

You report to the ICO within 48 hours of the parent telling you

**

Managing a data breach

A staff member downloads pupil **safeguarding information** onto a **memory stick** and **loses it** but **doesn't tell you**

The first you hear about it is when the parent concerned tells you people have been **talking about her child's safeguarding history on Facebook** for the **last 10 days** or so

You report to the ICO within **48 hours** of the parent telling you

Managing a data breach

What do you think the ICO response will be?

1. Thank you for reporting it
2. Issue a formal warning
3. Fine you up to £75,000
4. Fine you more than £75,000

Managing a data breach

72 hours is your longstop

First report in within a matter of hours with updates to follow

Time critical...

Fast, efficient and complete reporting could be the difference between a £20,000 fine and a £100,000 fine

Managing a data breach

- ICO checklists

Preparing for a personal data breach

- We know how to recognise a personal data breach
- We understand that a personal data breach isn't of personal data.
- We have prepared a response plan for addressing breaches that occur.
- We have allocated responsibility for managing breaches to a dedicated person or team.
- Our staff know how to escalate a security incident to the appropriate person or team in our organisation to determine whether a breach has occurred.

Responding to a personal data breach

- We have in place a process to assess the likely risk to individuals as a result of a breach.
- We know who is the relevant supervisory authority for our processing activities.
- We have a process to notify the ICO of a breach within 72 hours of becoming aware of it, even if we do not have all the details yet.
- We know what information we must give the ICO about a breach.
- We have a process to inform affected individuals about a breach which is likely to result in a high risk to their rights and freedoms.
- We know we must inform affected individuals without undue delay.
- We know what information about a breach we must provide to individuals, and that we should provide advice to help them protect themselves from its effects.
- We document all breaches, even if they don't all need to be reported.

Managing a data breach

What must you tell the ICO?

1. Nature of the breach and where possible
 - a. Categories and number of data subjects concerned
 - b. Categories and number of personal data records concerned
2. Name and contacts details of your DPO
3. Describe likely consequences of the data breach

Managing a data breach

What must you tell the ICO (cont.)?

4. Describe measures taken/to be taken to address the breach and mitigate possible adverse affects

You can provide this information in stages, but without undue delay

What does this look like in practice?

**

Managing a data breach

In practice

- Drop everything - akin to a serious safeguarding incident
- Follow your data breach procedures
- Seek external legal support as appropriate
- Business critical priority to manage quickly and effectively

Managing a data breach

- Crisis management
 - Who is in your team?
 - What gaps do they leave behind?
 - Who does what?
 - Who leads?
 - Where do you meet?

Summary

- Hefty fines
- DPO role is to lead on breach management
- Define your team and their roles
- Get to know the breach report form inside out



Please note

The information contained in these notes is based on the position at May 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.

© Browne Jacobson LLP 2018. Browne Jacobson LLP is a limited liability partnership.

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

Effectively managing a data breach

ensure breaches are known, managed and remedied immediately, when to advise the ICO and reporting the right information quickly to reduce any potential fine

Dai Durbridge

Browne Jacobson LLP

Changing your school's culture

working with your staff to understand risk, working practices that need to change and how to successfully influence change to ensure GDPR compliance

Dai Durbridge

Browne Jacobson LLP

Status update!

Data audit?

Policies, procedures and documents updated?

DPO appointed and a long way towards being suitably trained

So by the end of today you are 80% of the way there...

25 May 2018

- The world will not end
- It is not a deadline - it's a start line
- Don't worry about it

- ...But greater public awareness, so culture change is critical

Changing culture

- The big final 20% is the culture change
- Not going to be achieved this academic year
- Need longer to win hearts and minds

Changing culture

- Accountability and compliance focus under GDPR
- “Keep it just in case” mantra
- Privacy and data security not at the forefront of minds

Tis important stuff...

Remember - fines of up to €20,000,000

Tis important stuff...

- South East Local Authority
- Police Force
- Local Authority (some years ago)

Changing culture

- Change management
- Expect resistance from (some) staff and plan for it
- Some behaviours need to stop, others need a tweak

Changing culture

- What behaviours need to change at your school?

* **

Changing culture

Some examples...

1. Use of USB pen drives - encrypted or not
2. Use of personal email addresses
3. Email to wrong recipient
4. Downloading on home computers
5. Email access on phones and tablets
6. Sharing personal data without password protecting
7. Leaving laptop/personal data in the car overnight

Changing culture

- What is your biggest risk?
- What is the quick win you can achieve first?
- Focus on achieving the objective not meeting an arbitrary timeframe

Changing behaviour

- A balance to be struck between changing behaviours and adding safeguards to existing behaviours
- Can't change behaviour overnight - needs to be done at the right time at the right pace in the right way
- Work with staff to influence change

Changing behaviour

- Don't mention GDPR
- Position it as changing working practices to make staff lives better:
 - Remote working
 - Not lugging documents around
 - Heightened security to protect their own hardware
- Consult, cooperate, communicate

Changing behaviour

- Help them with new skills
 - How to guides
 - Top tips
 - Do it for them!

- Remember -outcome is more important than timeframe

Summary

- Some behaviours needs to stop, other need a change
- Work with your staff to influence positive change
- Will need SLT support and leadership to succeed
- Expect some challenge...

Final questions and wrap up

Please note

The information contained in these notes is based on the position at May 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.

© Browne Jacobson LLP 2018. Browne Jacobson LLP is a limited liability partnership.



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

Please note

The information contained in these notes is based on the position at May 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.

© Browne Jacobson LLP 2018. Browne Jacobson LLP is a limited liability partnership.



Daljit Kaur | 0330 045 2281
daljit.kaur@brownejacobson.com

DPO Foundation Training

Dai Durbridge and Daljit Kaur

Browne Jacobson LLP