John Walker, Solicitor
www.schoolslegalsupport.co.uk
07736669961
john@jawalker.co.uk

Data Protection and GDPR Training for Schools

These slides and the content of the course do not constitute legal advice. They are general training materials. No case comments in the training should be taken as legal advice and no solicitor client relationship is formed from any such comments and discussion. Advice about specific issues should be obtained separately.

Course Content

Learning Objectives

To understand obligations of the GDPR

To identify differences between the DPA and GDPR frameworks

To clarify data processing obligations and responsibilities

To prepare the school for implementation and possible breaches

To understand the legal framework - how it fits with other obligations

To consider the practical impact in school

To ensure that data protection is on everyone's radar

What is the GDPR?

- A complete overhaul of Data Protection legislation. The DPA came into law in 1998, a lifetime ago.
- An EU Directive - to strengthen arrangements for security and safety of data held within an organisation – which includes schools.

Why does it matter?

- "The GDPR replaces the DPA and affects all UK companies who collect or process personal information. It's focused on looking after the privacy and rights of the individual, and based on the premise that consumers and data subjects should have knowledge of what data is held about them and how it's used."

Steve Sands, Chief Information Security Officer (CISO) and Data Protection Officer (DPO) at Synectics Solutions.

When does it come into force?

25th May 2018

How is it different?

Data Protection Principles – the DPA

Personal data must be:-	Fairly and lawfully processed	Obtained for one or more specified purposes and not used for any other purpose
Adequate, relevant and not excessive	Accurate	Not kept for longer than is necessary
Processed in line with the data subject's rights	Kept secure; and	Not transferred to countries without adequate protection (i.e. outside the EEA).

Who processes data in your school?

- Nearly everyone – and under the GDPR EVERYONE is responsible for good data management and processing.
- The Data Controller is the head/governing body or Academy Trust
- A Data Protection Officer needs to be appointed – with a job description and authority as required.
- Everyone who accesses a child or staff members' data is a data processor

And I mean EVERYONE

Processing personal data - common issues

- Practicalities
- Fair processing notice required on, e.g. website / student enrolment forms / job application forms
- Systems needed to record consent (and lack of it) and any changes to it
- Contents of notice
- Photographs
- CCTV
- Safeguarding

Key Principles – Article 5 personal data shall be:

(a) processed lawfully, fairly and in a transparent manner in relation to individuals;

(b) collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall not be considered to be incompatible with the initial purposes;

(c) adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed;

(d) accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay;

(e) 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; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes subject to implementation of the appropriate technical and organisational measures required by the GDPR in order to safeguard the rights and freedoms of individuals;

(f) 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.

Article 5(2) requires that

- “the controller shall be responsible for, and be able to demonstrate, compliance with the principles.”

Lawful Processing

For processing to be lawful under the GDPR, you need to identify a lawful basis before you can process personal data. These are often referred to as the "conditions for processing" under the DPA.

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 take steps to enter into a contract

6(1)(c) – Processing is necessary for compliance with a legal obligation

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 pursued by the controller or a third party, except where such interests are overridden by the interests, rights or freedoms of the data subject.

Consent

Consent under the GDPR must be a freely given, specific, informed and unambiguous indication of the individual's wishes. There must be some form of clear affirmative action – or in other words, a positive opt-in – consent cannot be inferred from silence, pre-ticked boxes or inactivity.

The process must be specific, granular, clear, prominent, opt-in, properly documented and easily withdrawn.

Rights for Individuals

- The right to be informed
- The right of access
- The right to rectification
- The right to erasure
- The right to restrict processing
- The right to data portability
- The right to object
- Rights in relation to automated decision making and profiling.

To be informed

- What information is held?
- Who holds it?
- Why is it held?
- Retention periods?
- That each data subject has rights. Consent can be withdrawn at any time (to some things).
- Right to complain
- https://www.gov.uk/government/publications/data-protection-and-privacy-privacy-notices

Right of Access

Under the GDPR, individuals will have the right to obtain:

- confirmation that their data is being processed;
- access to their personal data;
- No fee (unless unreasonable or multiple request)
- Provide information within a month, but an extension to two months is possible – school holidays for example
- Can supply by electronic means
- If there is a lot of information you can ask the person to be more specific

Rectification

- Individuals are entitled to have personal data rectified if it is inaccurate or incomplete.

- If you have disclosed the personal data in question to third parties, you must inform them of the rectification where possible. You must also inform the individuals about the third parties to whom the data has been disclosed where appropriate.
- Respond within a month, can be extended to two.
- If you refuse to amend you have to tell them why and explain complaint/appeal available

Right to Erasure

The right to erasure does not provide an absolute ‘right to be forgotten’. Individuals have a right to have personal data erased and to prevent processing in specific circumstances:

Where the personal data is no longer necessary in relation to the purpose for which it was originally collected/processed.

When the individual withdraws consent.

When the individual objects to the processing and there is no overriding legitimate interest for continuing the processing.

The personal data was unlawfully processed (ie otherwise in breach of the GDPR).

The personal data has to be erased in order to comply with a legal obligation.

The personal data is processed in relation to the offer of information society services to a child.

Refuse Erasure

You can refuse to comply with a request for erasure where the personal data is processed for the following reasons:

- to exercise the right of freedom of expression and information;
- to comply with a legal obligation for the performance of a public interest task or exercise of official authority.
- for public health purposes in the public interest;
- archiving purposes in the public interest, scientific research historical research or statistical purposes; or
- the exercise or defence of legal claims.

Children's Data

How does the right to erasure apply to children's personal data?

- There are extra requirements when the request for erasure relates to children's personal data, reflecting the GDPR emphasis on the enhanced protection of such information, especially in online environments.
- If you process the personal data of children, you should pay special attention to existing situations where a child has given consent to processing and they later request erasure of the data (regardless of age at the time of the request), especially on social networking sites and internet forums. This is because a child may not have been fully aware of the risks involved in the processing at the time of consent (Recital 65).

Right to restrict processing

When processing is restricted, you are permitted to store the personal data, but not further process it. You can retain just enough information about the individual to ensure that the restriction is respected in future.

- Where an individual contests the accuracy of the personal data, you should restrict the processing until you have verified the accuracy of the personal data.
- Where an individual has objected to the processing (where it was necessary for the performance of a public interest task or purpose of legitimate interests), and you are considering whether your organisation's legitimate grounds override those of the individual.
- When processing is unlawful and the individual opposes erasure and requests restriction instead.
- If you no longer need the personal data but the individual requires the data to establish, exercise or defend a legal claim.

Portability

- The right to data portability allows individuals to obtain and reuse their personal data for their own purposes across different services.
- It allows them to move, copy or transfer personal data easily from one IT environment to another in a safe and secure way, without hindrance to usability.
- Not really an issue for schools!

Right to object to processing

Individuals have the right to object to:

- processing based on legitimate interests or the performance of a task in the public interest/exercise of official authority (including profiling);
- direct marketing (including profiling); and
- processing for purposes of scientific/historical research and statistics.

But you can process if:

- you can demonstrate compelling legitimate grounds for the processing, which override the interests, rights and freedoms of the individual; or
- the processing is for the establishment, exercise or defence of legal claims.

Automated decision making and profiing

The GDPR provides safeguards for individuals against the risk that a potentially damaging decision is taken without human intervention.

Not relevant for schools

Accountability

You MUST demonstrate how you comply

Set out your:-

- Technical measures, audit, staff training and reviews of policies
- Maintain relevant documentation of data processing - how, why and when
- Appoint a Data Protection Officer
- BYOD
- Staff and pupil data security – supply teachers and temporary staff
- CCTV policy

Data Protection Impact Assessments

You must carry out a DPIA when:

- using new technologies; and
- the processing is likely to result in a high risk to the rights and freedoms of individuals.
- Large scale, systematic monitoring of public areas (CCTV).

- Other examples are not relevant to schools

What to include in a DPIA

- A description of the processing operations and the purposes, including, where applicable, the legitimate interests pursued by the controller.
- An assessment of the necessity and proportionality of the processing in relation to the purpose.
- An assessment of the risks to individuals.
- The measures in place to address risk, including security and to demonstrate that you comply.

Data Protection Officer

- Public bodies - so all schools – must appoint a DPO
- The DPO reports to the highest management level of your organisation – ie board level.
- The DPO operates independently and is not dismissed or penalised for performing their task.
- Adequate resources are provided to enable DPOs to meet their GDPR obligations.
- Can be outsourced and shard across organisations
- Codes of conduct are available and endorsed by GDPR

Breaches

- A personal data breach means a breach of security leading to the destruction, loss, alteration, unauthorised disclosure of, or access to, personal data. This means that a breach is more than just losing personal data.
- You only have to notify the relevant supervisory authority of a breach where it is likely to result in a risk to the rights and freedoms of individuals. If unaddressed such a breach is likely to have a significant detrimental effect on individuals – for example, result in discrimination, damage to reputation, financial loss, loss of confidentiality or any other significant economic or social disadvantage.

Telling the individual

- Where a breach is likely to result in a high risk to the rights and freedoms of individuals, you must notify those concerned directly.
- A ‘high risk’ means the threshold for notifying individuals is higher than for notifying the relevant supervisory authority.

What do I include?

The nature of the personal data breach including, where possible:

- the categories and approximate number of individuals concerned; and
- the categories and approximate number of personal data records concerned;
- The name and contact details of the data protection officer (if your organisation has one) or other contact point where more information can be obtained;
- A description of the likely consequences of the personal data breach; and
- A description of the measures taken, or proposed to be taken, to deal with the personal data breach and, where appropriate, of the measures taken to mitigate any possible adverse effects.

How do I notify?

- A notifiable breach has to be reported to the relevant supervisory authority within 72 hours of the organisation becoming aware of it. The GDPR recognises that it will often be impossible to investigate a breach fully within that time-period and allows you to provide information in phases.
- If the breach is sufficiently serious to warrant notification to the public, the organisation responsible must do so without undue delay.
- Failing to notify a breach when required to do so can result in a significant fine up to 10 million Euros or 2 per cent of your global turnover.

Data Transfer out the EU

- Check where your data is stored

- Cloud servers
- Online provision
- Emails

- Check and ask the provider how do they comply and get a signed contract or SLA.

GDPR - Contracts with 3rd Parties

- **28(3)** Processing by a processor must be governed by a contract that is binding on the processor with regard to the controller and that sets out the subject-matter and duration of the processing, the nature and purpose of the processing, the type of personal data, categories of individuals whose data is being processed and the obligations and rights of the controller. The contract must stipulate, in particular,

that the processor will:

- **28(3)(a)** process only on documented instructions, including regarding international transfers(unless, subject to certain restrictions, legally required to transfer to a third country or international organisation);
- **28(3)(b)** ensure those processing personal data are under a confidentiality obligation(contractual or statutory);

- **28(3)(c)** take all measures required under the security provisions (Article 32) which includes pseudonymising and encrypting personal data as appropriate;
- **28(3)(d)** only use a sub-processor with the controller's consent (specific or general, although where general consent is obtained processors must notify changes to controllers, giving them an opportunity to object);
- flow down the same contractual obligations to sub-processors;
- **28(3)(e)** assist the controller in responding to requests from individuals (data subjects) exercising their rights;
- **28(3)(f)** assist the controller in complying with the obligations relating to security, breach notification, DPIAs and consulting with supervisory authorities (Articles 32-36);
- **28(3)(g)** delete or return (at the controller's choice) all personal data at the end of the agreement (unless storage is required by EU/member state law);
- **28(3)(h)** make available to the controller all information necessary to demonstrate compliance; allow/contribute to audits (including inspections); and inform the controller if its instructions infringe data protection law.

Information Sharing

- Advice for practitioners providing safeguarding services to children, young people, parents and carers
- March 2015

CURRENT DFE GUIDANCE

Summary

- Information sharing is vital to safeguarding and promoting the welfare of children and young people. A key factor identified in many serious case reviews (SCRs) has been a failure by practitioners to record information, to share it, to understand its significance and then take appropriate action.

Sharing Information

Sharing information is an intrinsic part of any frontline practitioners' job when working with children and young people. The decisions about how much information to share, with whom and when, can have a profound impact on individuals' lives. It could ensure that an individual receives the right services at the right time and prevent a need from becoming more acute and difficult to meet. At the other end of the spectrum it could be the difference between life and death.

Fears about sharing information cannot be allowed to stand in the way of the need to safeguard and promote the welfare of children at risk of abuse or neglect. No practitioner should assume that someone else will pass on information which may be critical to keeping a child safe.

Refusing a SAR

When a SAR comes in, you need to consider it might be appropriate to withhold information if:

- information that might cause serious harm to the physical or
- mental health of the pupil or another individual;
- information that would reveal that the child is at risk of abuse,
- where disclosure of that information would not be in the child's best interests;
- information contained in adoption and parental order records;
- and certain information given to a court in proceedings concerning the child.

Guidance

- All information sharing decisions and reasons must be recorded in line with your organisation or local procedures.
- If at any stage you are unsure about how or when to share information, you should seek advice and ensure that the outcome of the discussion is recorded.
- If there are concerns that a child is suffering or likely to suffer harm, then follow the relevant procedures without delay.

The Children Act 1989

Section 47 of the Children Act 1989 places a duty on local authorities to make enquiries where they have reasonable cause to suspect that a child in their area may be at risk of suffering significant harm. Section 47 states that unless in all the circumstances it would be unreasonable for them to do so, the following authorities must assist a local authority with these enquiries if requested, in particular by providing relevant information:

- any local authority;
- any local education authority;
- any housing authority;
- any health authority;
- any person authorised by the Secretary of State

The Children Act 2004

Section 10 of the Act places a duty on each children's services authority to make arrangements to promote co-operation between itself and relevant partner agencies to improve the well-being of children in their area in relation to:

- Physical and mental health, and emotional well-being;
- Protection from harm and neglect;
- Education, training and recreation;
- Making a positive contribution to society;
- Social and economic well-being.

Children Act 2004 – Section 11

Organisations who have a duty to have arrangements to safeguard and promote the welfare of children are:

- the local authority;
- NHS England;
- clinical commissioning groups;
- NHS Trusts, NHS Foundation Trusts;
- the local policing body;
- British Transport Police Authority;
- Prisons;
- National Probation Service and Community Rehabilitation Companies;
- youth offending teams; and
- bodies within the education and /or voluntary sectors, and any individual to the extent that they are providing services in pursuance of section 74 of the Education and Skills Act 2008.

Education Act 2002

Section 175 Duties of LEAs and governing bodies in relation to welfare of children.

(1)A local education authority shall make arrangements for ensuring that the functions conferred on them in their capacity as a local education authority are exercised with a view to safeguarding and promoting the welfare of children.

(2)The governing body of a maintained school shall make arrangements for ensuring that their functions relating to the conduct of the school are exercised with a view to safeguarding and promoting the welfare of children who are pupils at the school.

(4)An authority or body mentioned in any of subsections (1) to (3) shall,… have regard to any guidance given from time to time by the Secretary of State or by the National Assembly for Wales.

Education Act 2002

In this section—.

- “child” means a person under the age of eighteen;
- “governing body”, in relation to an institution within the further education sector, has the meaning given by section 90 of the Further and Higher Education Act 1992 (c. 13);
- “maintained school” means a community, foundation or voluntary school, a community or foundation special school or a maintained nursery school.
- **The same duty applies to independent schools (which include Academies and free schools) by virtue of regulations made under section 157 of the same Act.**

Pupil Records – Education Act 1996

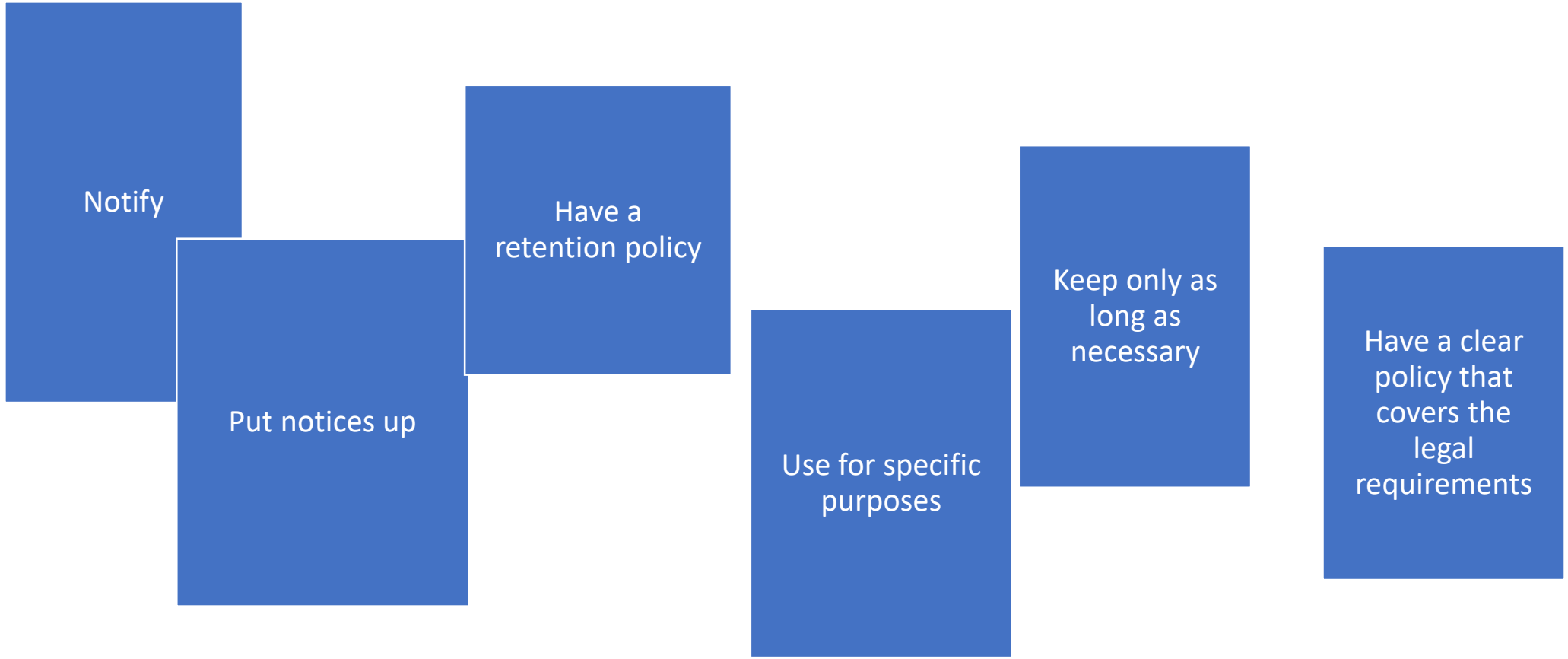
- If a SAR is made for information containing, in whole or in part, a pupil's 'educational record', a response must be provided within 15 school days. The maximum amount you may charge for dealing with the request depends on the number of pages of information to be supplied.

The Data Protection (Subject Access Modification) (Education) Order 2000/414

- Exemptions from section 7 (general disclosure under the DPA)

- 5.—(1) Personal data to which this Order applies are exempt from section 7 in any case to the extent to which the application of that section would be likely to cause serious harm to the physical or mental health or condition of the data subject or any other person.

CCTV and Data Protection



BYOD and data security

- Encryption - critically important

In 2009, A barrister breached the data protection act by failing to encrypt A laptop containing sensitive personal data.

- The laptop contained personal data relating to a number of individuals involved in multiple court cases the barrister had been working on. This included details relating to the physical and mental health of persons involved in two of the cases. The laptop was later stolen from the barrister's home when she was away on holiday. Whilst the barrister had a number of security measures in place at the time of the theft, the ICO found that she failed to ensure that either the device or the sensitive information stored on it was appropriately encrypted.

How to prepare – ASCL and the ICO

- Awareness: ensure decision makers and key individuals in your school or college are aware that the DPA is changing to the GDPR. They need to appreciate the impact it will have and how the new legislation will affect your institution.
- Information you hold: organise an information audit and document the personal staff and student data you currently hold, where it came from and who it is shared with.
- Communicating privacy information: review your current privacy guidance and put a plan in place for making any necessary changes in good time.

- Individuals’ rights: check your current procedures to ensure they cover all rights of individuals, including how personal data is deleted, or how data is provided electronically.
- Subject access requests: update your procedures, plan how you will handle requests within the new timescales and provide any additional information.
- Legal basis for processing personal data: review the various types of data processing you carry out, identify and document your legal basis for carrying it out .
- Consent: review how you are seeking, obtaining and recording consent and whether any changes are required.
- Students: start thinking what systems you are going to put in place to verify individuals’ ages, and to gather parental or guardian consent for the data processing activity.

- Data breaches: ensure you have got the right procedures in place to detect, report and investigate a personal data breach.

- Data protection by design and data protection impact assessments: consider when to begin implementation of the Privacy Impact Assessments at your school.

- Data Protection Officers: designate a data protection officer or an individual to take responsibility for data protection compliance.

- International considerations: consider the implications for those organisations with international operations.

Compliance Checklist

- Notification
- Data Protection Principles
- Fair processing
- Security
- Disposal
- Policies
- Subject access requests
- Data sharing
- Websites
- CCTV
- Photographs
- Third party processing
- Training