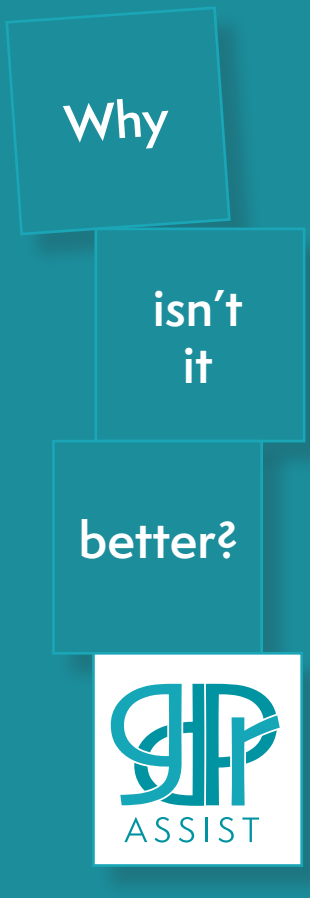
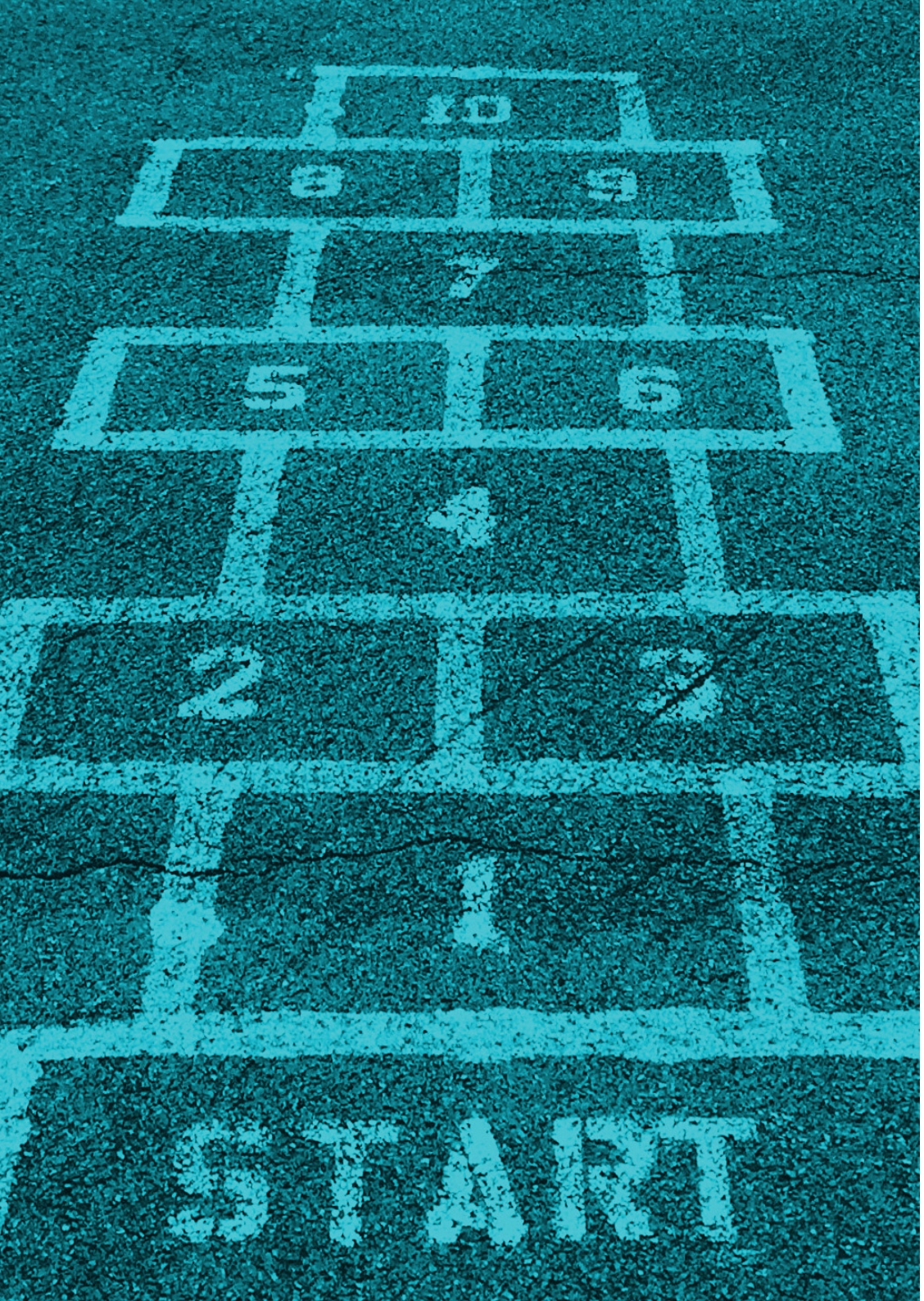
GDPR Compliance in Schools



A discussion white paper by
Paul Strout, Owner and
Chief Consultant, GDPR Assist



Contents

Introduction

The General data Protection Regulations (GDPR) came into effect 1 year ago on 25th May 2018. In the months preceding GDPR there was much talk of the impact it would have and the compliance work required for organisations in both the public and private sectors. There was also a large amount of misinformation and misunderstanding of the practical impact GDPR would have on the routine operations of businesses and public services.

In the year since the onset of GDPR the Information Commissioner's Office (ICO) have undertaken a number of audit and advisory visits:

28% of ALL ICO audits & advisory visits are to schools & colleges [1]

Main areas of concern highlighted are:

- Governance & Accountability
- Training & Awareness
- Data Sharing

The updating of data protection legislation, and consequential increase in resourcing for the ICO, come at a time of increasing public awareness of the value of personal information and risks associated with its processing. Media coverage of significant data breaches and questionable practices by social media and search businesses have helped increase the perception that the public have of the importance of personal data and how organisations are using their data to target them with commercial and political advertising.

The specific purpose of this document is to spur further discussion amongst senior leaders within schools and colleges, to ask two key questions, and to posit potential answers. For educational leaders the two questions are:

- Why are we falling short of complying with the regulations?
- What can be done within the school to change this?

[1] *138 visits since May 25th 2018, 39 to schools and colleges (https://ico.org.uk/action-weve-taken/audits-advisory-visits-and-overview-reports/)*

The potential third question would be "why is this important?". The clear answers to that question are:

- Education is one of the largest processors of personal data in the UK (alongside health); virtually the entire population has been a pupil or parent, or will be one,
- In addition to being the collective custodians of very large data sets, schools are also processing data which are often sensitive, include special category information, and that present a high risk to the individual in the event of a breach,
- As the curriculum develops and pupils are taught the value of personal data, the importance of online privacy, and the dangers that can exist in a highly connected society it is incumbent on their educators to demonstrate their responsibility and show that the trust placed in them is justified,
- In a modern compensation culture claims against schools and colleges for breaching data protection legislation could carry significant cost, not just in terms of financial settlement but also in the resources needed to investigate and resolve future claims,
- Reputational damage to schools can impact not only the establishment itself but the leadership teams involved,
- In an under-funded, under-resourced area of public service it is better to spend a little now rather than risk a lot later,
- And finally – it is your legal duty to do so.

ASSIST

Current State of Compliance in Schools

In a recent survey of GDPR compliance in schools *(GDPR in UK Schools* [2] *& Colleges – RM – April 2019)* 52% of respondents self-declared that their school was not compliant. Another startling statistic from the same report was that 91% of respondents believed that their schools knew where all their data exists, including those items held by third parties; given the complexity and uncertainty of cloud storage locations, the huge amount of data stored in both paper and digital media within a typical school, and the lack of compliance then this statistic is misleading at best and points to a wider issue of unconscious ignorance.

It is also worth noting that the majority of respondents to the survey were IT Managers and only a small percentage were part of the senior leadership team. This would suggest that the perception of compliance came from a systems perspective rather than a process and awareness perspective and would also be highly likely to be limited to the storage and processing of digital records and less likely to cover paper based processes. I would propose that the likely figure for non-compliance, should a wider audience be canvassed, would be significantly higher than 52%.

REASONS FOR NON-COMPLIANCE

In discussions with schools, and with fellow data protection professionals, the following reasons are most often cited as being the cause for the current lack of effective compliance programmes within schools and colleges:

- Lack of direction from governors [3] and SLT,
- Lack of specialist knowledge,
- Lack of awareness amongst departmental leadership and wider staff,
- Lack of resources (people) and money.

In addition there appears to have been a trend of attempting to appear compliant through some tactical measures such as revising the school's privacy policy using the DfE templates (Data Protection: a toolkit for schools – Department for Education – August 2018) and appointing a Data Protection Officer (often outsourced) without necessarily devoting the resources to create an ongoing effective data protection programme within the school.

To address the four points specifically:

LEADERSHIP (GOVERNORS AND SLT)

Who has responsibility for data protection amongst the governing body? It would appear that the role where it is assigned is often given to the person also providing governorship for safeguarding. Whilst this would initially appear to be justifiable it is highly probable that these are different areas of knowledge and skill, and that the data protection duties are likely to assume a secondary priority to the more pressing needs of physical and psychological safeguarding.

Within the SLT the picture is more mixed, and there doesn't appear to be a clear norm for assigning this responsibility. In fact it frequently gets delegated to a Business Manager, Bursar, or IT Manager.

Schools must appoint a Data Protection Officer. This can be a member of staff (and can be an additional duty) or an outsourced professional. However it is imperative that the staff member must be suitably skilled, functionally independent, have direct access to leadership, and have no conflict of interest (for example it would be inappropriate to pass DPO responsibility to anyone responsible for expenditure decisions). Where an external body is appointed as a DPO the school should ask the key question of why they have chosen this route, and how the DPO is going to actively enable the school's compliance programme. If the answer to the first question is simply "to comply", with no following active engagement then this would appear to be not compliant in itself.

If there is no clear leadership ownership and direction for an ongoing compliance programme then it is highly likely that compliance will remain in its current state, thus exposing the school, its staff and its pupils to significant risk.

[2] *https://www.rm.com/pdf/web/viewer.html?file=~/media/PDFs/Whitepapers/GDPR-in-Schools_RM-Education.pdf*

[3] *Whilst this document refers to governors the comments are equally valid for trustees of an academy*

SPECIALIST KNOWLEDGE

There is a lack of accurate and up to date knowledge of GDPR and related regulations within schools. Whilst online resources exist from the DfE (Data Protection: a toolkit for schools – Department for Education – August 2018) and ICO, the DfE toolkit is still in its draft 1.0 beta version and not all of the ICO content (available at ico.org.uk) for education has been updated from the advice given under the Data Protection Act 1998.

Furthermore it is debatable whether many of the provided templates for documents such as Privacy Notices effectively meet the requirements for transparency within GDPR. A core requirement for transparency to be effective is that the information should be "easily accessible and easy to understand, and that clear and plain language is used" *(GDPR Recital 39)*. This is especially important when the level of literacy skills amongst pupils and their parents [4] is also taken into account – a privacy notice should inform, one that has a structure more akin to a set of terms and conditions is therefore of questionable value. This point highlights the need for school staff to be actively engaged in the process of constructing documentation as their education skills can be applied to improve transparency provided they have access to specialist GDPR knowledge.

STAFF AWARENESS

Some schools have implemented GDPR training to a limited extent, perhaps by running a workshop around the time of implementation last May, however there is a lack of an ongoing awareness programme including less formal cascades and updates.

Induction processes for new staff are also lacking in updates and frequently still refer to the pre-existing regime of the DPA 98, whilst staff exit processes often miss the topic entirely.

A lack of specialist knowledge, and access to reliable resources, combined with a lack of ownership amongst the governance and leadership functions result in a lower than optimal staff awareness.

[4] *The International Survey of Adult Skills 2012: adult literacy, numeracy and problem solving skills in England – 49.5% of adults in England display literacy skills at OECD level 2 or lower.*

In addition procuring external resources to conduct staff awareness training can be costly and not always optimised for the school environment. It is also worth remembering that awareness is an ongoing programme – not a one-off event.

LACK OF RESOURCES

There is a belief that compliance can only be achieved by expenditure on systems, software, training and staff.

Whilst it is true that compliance does incur cost it is not necessarily the case that a technology spend is either necessary or sufficient to achieve it.

In an under-funded, under-resourced sector such as education (both at the school level, and perhaps even greater at the college level) it is hardly surprising that data protection compliance has lost out to more urgent needs for investment.

External advice and consultancy are typically expensive (>£1,000 per day) and unpredictable in terms of overall cost. *One area which should be investigated though is whether the outsourced DPO provider is delivering an active compliance programme for the school, or whether there could perhaps be a better way of achieving this from that budget.*

If the issues around governance/leadership are addressed then data protection compliance can be recognised for the vital issue that it is and appropriately resourced and prudently budgeted for.

Making Positive Change

Having discussed the current state of compliance within schools and colleges, and looked at some of the more common reasons for this, this section looks at some of the key steps which the organisation can take to introduce an active programme to minimise the risks faced by non-compliance and demonstrate good data ethics.

MAKE A LEADERSHIP DECISION

Assign Data Protection as a responsibility within the governing board and senior leadership team. Where additional skills are required consider providing suitable training for the individuals to GDPR Foundation level as a minimum.

Ensure that Data Protection is a permanent agenda item in governance and SLT meetings.

Ensure that Data Protection issues are included on risk registers to be addressed by the governing body and SLT.

Review the decision around the appointment of your Data Protection Officer. You have an obligation to appoint a DPO, but the individual must not only be suitably qualified but must also play a pro-active role in your compliance programme. Evaluate whether it would be more cost effective to bring the role in-house, or whether another provider would deliver the required pro-active support.

ASSIGN TASKS

The SLT should then, under guidance from the nominated Data Protection Lead and DPO, address the following key tasks. The work required to complete the tasks should involve members of the wider school staff – not only to spread the workload but also to also encourage wider staff awareness:

- Public website – cookie control and privacy notice
  - Is the cookie control effective and defaulted to not deploy cookies which collect personal data?
  - Is the privacy notice fit for purpose? Does it reflect you as a school and, above all, is it likely to be read and understood?
- Staff Awareness
  - Design a rolling programme of staff awareness
  - Appoint Data Protection champions within departments
  - Decide how to do face-to-face training (buy it in? Use in-house skills? Use your DPO?)
  - Decide how other information sources can help: intranet, newsletters, e-bulletins, etc.

- Records of Processing
  - Collate your GDPR Article 30 records of processing
  - Chose a template and stick to it
  - Ask your DPO for guidance
- Data Protection Impact Assessments (DPIA)
  - Take your completed Article 30 records and assess each data process against the criteria for the requirement to perform a DPIA. Ask your DPO for guidance or see the advice on ico.org.uk
  - Contact suppliers acting as Data Processors for their help in furnishing information for the DPIA
  - Where required complete the DPIAs and rate the level of risk
  - Prioritise the highest risk DPIAs for action, report these on the risk register and for debate by the SLT and governing body for further corrective action (tolerate, treat, terminate or transfer) – again, your DPO should be guiding this activity

Conclusion

Whilst the state of compliance amongst schools and colleges in the UK would appear to be patchy at best it is clear that with a will and the support of the leadership team the position can be significantly improved.

Having access to friendly advice and help is key – this may need additional skills at the leadership/governance level or a review of your DPO provision.

Risks an be mitigated better by a change of culture and activity than by the deployment of technology.

There is no certification for GDPR compliance, indeed it is a valid point of view to say that organisations can never confidently state their compliance as the data environment it relates to changes so frequently – however demonstrating your commitment to the compliance journey is both a legal requirement and an ethical stance to take.

About GDPR Assist

GDPR Assist is the trading name of Paul Strout, a Bury based Data Protection Practitioner with many decades experience in helping organisations with their key operational processes.

More information is available at **www.gdprassist.co.uk**