Freshers: from vulnerable children to adults at risk? What schools and universities need to know about the transfer of safeguarding information between institutions

Kathleen Heycock | January 2017

It is well-recognised that vulnerable children can slip off the safeguarding radar when leaving school, and that the line between a 17 and an 18 year old is largely an arbitrary one. It is also true that a transition to the "big wide world" of higher education can be a watershed moment in a vulnerable child's life combining a sense of trepidation and new adventure: tumultuous and disconnecting for some, yet a chance for a fresh start for others. Many may want to leave troubled school years behind them. But what are the roles, and mutual responsibilities, of schools and universities when a pupil about whom there are safeguarding concerns transitions into higher education?

> "What is lacking is a sweep-up set of rules, guidance or support infrastructure that governs the transition from a child in education to a young adult in education."

1. The gap in guidance and the need for a policy

There is ample guidance and information on what should be shared between schools when a child with safeguarding needs leaves one school to join another school, not least in the statutory guidance Keeping Children Safe in Education (KCSIE). But what if, for example, a pupil on the cusp of going to university is known to be a suicide risk or to have a drug or alcohol problem? This is a child in whom a school may have invested hours of care and attention and who has had significant support and a safety net available to them at all times. Schools understandably are very nervous to see that child, probably now legally an adult, walk away from that support and safety net – and any direct support provided by their family – with no-one at the university they are about to attend aware of their situation.

This is a very real concern to many schools but is something that few UK universities (as far as we are aware) have addressed. Clearly, this does not form part of the information provided at the application stage – and schools, parents and pupils would be very reluctant for it to be so. But is there a time and place for this information to be shared and how do you decide what is relevant? What and how much safeguarding information can, and/or should, be passed on?

Unfortunately, clear, easy-to-follow rules or directly applicable statutory guidance do not exist when it comes to sharing medical, mental health and other safeguarding information between schools and universities.

We have useful comparable or analogous material, such as KCSIE, provisions under the Care Act 2014 for safeguarding adults at risk, and the Government's Guidance on Information Sharing for Safeguarding Practitioners, which will cover certain scenarios. There is also a growing body of guidance available to universities on student mental wellbeing during their time in higher education (such as a Good Practice Guide produced by Universities UK in February 2015, and the JISC Code of Practice for supporting students). Some of the campus care culture from the United States, which is generally held to be more pastoral in outlook than higher educational institutions in the UK, appears to be reaching these shores – including in digital support solutions for students.

What is lacking is a sweep-up set of rules, guidance or support infrastructure that governs the transition from a child in education to a young adult in education.

In addition, it may not always be clear-cut that such a young adult may potentially be an adult at risk (within the legal definition), even though the sharing of certain information with the appropriate person at a university – assuming that role is clearly defined – might be in that person's best interests. Historically, designated safeguarding leads (DSLs) and the equivalent for adults at risk, Designated Adult Safeguarding Manager (DASM) at higher education institutions may not have always had the support, access or clearly-defined role that DSLs now have in schools. This leads to uncertainty as to with whom at the university a school should share the information, and what the university should then do with it.

2. Information sharing: the law

There is however an overall statutory regime which is relevant – and that is the Data Protection Act 1998 (due to be replaced and updated by new regulation in May 2018). The penalties for breaches of this Act (the DPA) are becoming more severe. However, with growing focus on when a university will have a duty of care to its students (see this recent article concerning three student suicides at Bristol University), there is also a strong legal liability imperative – quite apart from a moral and pastoral one – to have a clear, reasonable and justifiable policy sharing the right information with the right people. The purpose is to help keep students safe and protected as they transition from vulnerable children to *potentially* young adults at risk.

Information sharing is one of the cornerstones of safeguarding, in any context. Matching up this imperative with data protection law is not absolutely straightforward, but it is less often a bar than many DSLs, DASMs and organisations believe. One overriding philosophy we are happy to endorse is that data protection law should never stand in the way of a person's safety, and should not be an excuse for avoiding a difficult conversation. Preliminary conversations can be had on a no-names basis that do not trouble the DPA, and in which professionals can satisfy themselves as to whether there is an issue which needs monitoring or addressing.

From there, grounds and exemptions do exist within the DPA that enable sharing of even sensitive personal data in circumstances where a person's vital interests are at stake – and there are other possible bases, with certain conditions and safeguards (including prevention of crime). Whilst the guidance provided by the DPA regulator, the Information Commissioner, is not especially permissive on the interpretation of these grounds, the question arises of which is the greater risk and liability for organisations: the DPA, where a marginal decision has been made in good faith, or where a failure to share information costs the life or welfare of a young adult?

If you require further information on anything covered in this briefing please contact Kathleen Heycock (kathleen.heycock@farrer.co.uk ; +44(0)203 375 7113); Owen O'Rorke (owen.o'rorke@farrer.co.uk; +44(0)203 375 7348) or your usual contact at the firm on 020 3375 7000. Further information can also be found on the Child Protection Unit page on our website.

A risk-averse view to data sharing is all too common, though it is understandable: the Information Commissioner has recently come into the spotlight in the sector (among schools and alumni bodies) because of taking a harder line in other areas such as fundraising. But that focus on mass data processing activities can be clearly distinguished from well-intentioned individual decisions as to information sharing.

Probably the greatest risk in information sharing, legally or professionally, would be to provide sensitive personal information about a vulnerable individual to the wrong person (internally or externally). But provided that an appropriate person is identified to share with, matters of fine professional judgment should not be an enforcement priority of the data protection regulator. Even if the sharing proves ultimately unnecessary or even has the wrong consequences, it is a defence to damages or distress claims under the DPA to show that reasonable care had been taken to comply with the relevant DPA requirement. With this in mind, data protection compliance should never outweigh the primary care concern.

That is not to say the DPA should be ignored; indeed, it acts as an important set of checks and balances which will minimise the chances of poor decision-making or careless error. To operate with the comfort that the DPA will broadly not be at odds with one's professional duty, that means at least being aware of the relevant considerations, applying them to the facts, and keeping a record of the reasons for the decision either to share or not to share.

This need to cut through the sometimes arcane legal background, and present something that staff can easily follow, is precisely why in our view both schools and universities should adopt their own policies – to fill the gap presently left by the lack of statutory guidance, and save DSLs and DASMs from having to pore over the (notoriously confusing) non-disclosure provisions in the DPA.

3. Checklist for sharing and drawing up a policy

The key questions for the **sharing party** (usually in this case the school) that should form part of the policy will be as follows:

- In what cases, and on what occasions, should we consider sharing information?
- What is the purpose for sharing the information?
  - Data protection law requires a lawful purpose for sharing. This purpose should be recorded, securely, as a matter of internal record.
  - If there is a clear purpose, consideration should be given as to what information is necessary to assist that purpose (for example, do any documents – let alone a whole file – need to be shared, or can a no-names conversation be held first); and
- Has the individual consented to the sharing, or is there any issue in seeking consent from them?
- If not consent, is there another legal justification for sharing?

- for *non-sensitive* personal data, such as contact data, it can be as simple as establishing a legitimate interest (of any party) to share that will outweigh any possible prejudice to the individual;

- for *sensitive* data, e.g. sexual life, criminal allegations or medically confidential data, it would require an additional condition to share without explicit consent, such as protecting a person's vital interests – whether of the child/young adult, or another person (for example any of their peers). Although the Information Commissioner's guidance suggests this is only for life-or-death situations, past Government guidance on information sharing has placed the threshold lower and many lawyers with an interest in safeguarding would agree that matters of substantial personal safety would qualify;

- If we are clear of the purpose and believe there are legal grounds to disclose on a 'names' basis, consider:

  - exactly what needs to be shared (for example should we consider redaction, minimisation or anonymisation of third parties);

  - with whom at the higher education institution (ideally this would be a trained DSL or DASM who has been properly identified); and

  - how should the school share the information – both to ensure data security and to put the DSL or DASM on notice of the stated purpose of sharing, reminding them of the confidentiality of the material and care that should be taken in storing or further sharing it.

This should all form part of a risk assessment in sharing or reaching out to universities. Breaching confidentiality is one of the potential risks to be managed and mitigated – but so of course is not sharing information that could be important.

For the **receiving party** (university), the key questions are:

- What is the purpose for which this information is being shared with us? Do we agree with it?

- Is the right person taking receipt, and are they properly trained and supported?

- Does the child/young adult concerned know we have the information? When is it appropriate to hold it without their knowledge – or specifically against their wishes?

- Does the university have the right infrastructure for processing the information appropriately, i.e.

  - clear definition of roles;

  - secure storage, filing and access protocols;

  - procedures on when to share and when to act?

- What are the risks and benefits, including to the student body as a whole, in this information – whether in holding it, or not accepting, recording, or acting on this information? In other words, when is it appropriate for the university pro-actively to take on a duty of care?

- How long should the university hold the information, and how much of it (particularly if, as months or years pass, it has not yet proven necessary or useful)?

- Have we, in fact, received all we need? Are there any other organisations or sources of information who could lawfully assist in building up the picture (families, carers, authorities, student bodies) – and what safeguards and protocols should we consider in doing so?

- Does the university need to do anything immediately?

There is a question for universities of when merely being in receipt of certain information places them under a specific duty of care. Assuming the university have the right infrastructure for supporting students generally (i.e. publications, intranet, applications, peer support networks and so on), it should be considered how the receipt of the information feeds into those processes and whether the circumstances require special measures or monitoring for an individual.

Summary

Duties of care do not stop dead when an organisation's charges reach a certain arbitrary age, or move from one institution to another. Communication is vital in safeguarding, so that different parties are not each holding different pieces of the jigsaw – namely, connected information about an individual that might keep them or others safe from harm. At the same time, good communication is targeted and considered: neither excessive nor overly cautious, but giving proper care, consideration and respect to the wishes and dignity of the individual in question, as well as dispassionately assessing their needs.

Although – or, perhaps, *because* – there is no prescriptive legal regime, we suggest the school and the university each have a policy for this situation. Where possible, in specific instances (i.e. when the school has a pupil they wish to share information about) the school and the university should speak to each other about concerns they may have about a child/young adult on a no-names basis first and, where possible, record a formal understanding between them. The right information can then be shared on a named basis further to that understanding – being sure again to keep a good, secure record of the reasons why.

This is not simply a question of best practice and demonstrating all-around care, but also in mitigating unseen legal issues and dangers to individuals. In practical terms, where government or statute does not provide for specific steps, it falls to schools and universities to forge the way and bring clarity to the area by reverting to sound and lawful principles.