3PB Cyber Law Series
Data protection for schools and higher education institutions

By Matthew Wyard
3PB Barristers

1. Slightly different from the topic envisaged at the end of part 2 of the cyber series, this article deals with two circumstances. Firstly, the right to access educational data via a subject access request (prompted by a recent issue in my caseload) and, secondly, the data protection obligations owed by further and higher education institutions ("HEIs") in situations of crisis on campus.

The right of access to 'education data'

Definitions

2. Before considering the right of access to education data it is important to understand what 'education data' is. Education data is defined (in respect of England and Wales) at paragraph 14 of schedule 3 to the Data Protection Act 2018 ("the 2018 Act") as:

   "a record of information which is processed by or on behalf of the proprietor of, or a teacher at, a school in England and Wales [and] relates to an individual who is or has been a pupil at the school, and originated from, or was supplied by or on behalf of, any of [the following]: (i) an employee of the local authority that maintains the school, (ii) a teacher or other employee at the school (including an educational psychologist engaged by the proprietor under a contract for services), (iii) the pupil to whom the record relates or (iv) a parent of the pupil."

3. "Schools" as defined at paragraph 14(3) means a maintained school, an Academy, an alternative provision Academy, an independent school, a non-maintained special school.

4. One exception to the above definition is found at paragraph 14(2) which explicitly excludes data "which is processed by a teacher solely for the teacher's own use".

5. Consequently, most of the data/personal information held by a school will fall into the category of education data.

Rights of access

6. Dependent on the type of school attended by a pupil there are two rights of access to education data:

    a. Firstly, the pupil's right to access their education data by way of subject access request under Article 15 of the UK GDPR; and

    b. Secondly, the parent's right of access to their child's 'education record[1]' under either:

        i. The Education (Pupil Information)(England) Regulations 2005[2]; or

        ii. The Pupil Information (Wales) Regulations 2011[3].

7. Requests under the aforementioned Regulations will be dealt with in a separate article, however, it is important to note the distinction between a pupil's right of access and a parents right of access. The distinction should not be underestimated as the information provided in response to the different types of request is different. In response to a pupil's subject access request a pupil is entitled to receive all of their personal data, including that which doesn't fall into the definition of an educational record. A parent is only entitled to a copy of their child's educational record. There are also different time limits to comply with a request. A subject access request must be responded to within one month, whereas a request for an educational record must be complied with within 15 school days.

Subject access request

8. Where a child is competent to make a subject access request, then they are entitled to do so. There are also two limited circumstances when a parent can make a subject access request on behalf of their child: (i) when a child is not competent to act on their own behalf and (ii) when a child gives consent.

9. In relation to competence, the ICO provides helpful guidance on when a child will generally be deemed competent to make a subject access request:

[1] Defined at paragraph 13 of schedule 3 to the 2018 Act, as being a record containing education data. This mirrors the definition contained at Reg3 of the Education (Pupil Information)(England) Regulations 2005.
[2] SI 2005/1437.
[3] SI 2011/1942.

"if they are able to understand (in broad terms) what it means to make a subject access request and how to interpret the information they receive."[4]

10. If the child is competent to make a subject access request then any parental requests purporting to be subject access requests should not be responded to unless the child consents. However, even if a competent child authorises another to make a subject access request on their behalf, you should not consider the child to be competent if it becomes clear that they are being pressured by a third party to give consent to make a request.

11. Where a child does give consent to another to make a subject access request, then the school should still take account of the duty of confidence owed to the child, any potential detriment to the child (or another) if information is, or is not, disclosed and, more obviously, it is important to check whether a parental requester does have parental responsibility for the child.

12. A school cannot charge a child (or, if appropriate, the child's parents) for complying with a subject access request and, regardless of school holidays and staff absences, schools must still comply with the statutory timescale for disclosure.

13. Insofar as exemptions are concerned, the exemptions that apply to other personal data also apply to education data. Additionally, there are two exemptions that apply solely to education data which can be found at paragraphs 18-19 of Schedule 3 to the 2018 Act:

    a. Schools are not required to disclose education data if that data is supplied in a report or other evidence given to a court and processed in the course of legal proceedings, where the court may withhold data in whole or in part from the data subject under its powers under the Family Procedure Rules 2010 (paragraph 18); and

    b. Where providing education data in response to a subject access request would be likely to cause serious harm to the physical or mental health of an individual (paragraph 19).

[4] https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/right-of-access//how-do-we-recognise-a-subject-access-request-sar/#children.

Crisis on campus: What to do in a state of student emergency?

14. Further and higher education institutions (for ease of reference referred to herein jointly as "HEIs"), regardless of designation, are data controllers in respect of personal data held on their student population. Regularly, the personal data held will also fall into the category of 'special category' personal data[5] within the meaning of Article 9(1) UK GDPR, for which processing is prohibited unless one of the exceptions applies.

15. Quite properly, HEIs get anxious when faced with requests from families for information in respect of which their children are the data subject. One situation in which requests for information can arise is where parents suspect that their child may be struggling emotionally whilst studying away from home and want to access information in a bid to either draw attention to their child's potential problems, or to help them.

16. The new Data Sharing Code of Practice ("the Code of Practice") issued by the Information Commissioner's Office ("the ICO") under section 125 of the Data Protection Act 2018 came into force on 05 October 2021 and offers guidance on this issue.

17. The Code of Practice provides:

> "In an emergency, you should go ahead and share data as is necessary and proportionate. Not every urgent situation is an emergency. An emergency includes:
>
> - preventing serious physical harm to a person;
> - preventing loss of human life;
> - protection of public health;
> - safeguarding vulnerable adults or children;
> - responding to an emergency; or
> - an immediate need to protect national security.
>
> … the UK GDPR and the DPA 2018 do not prevent you from sharing personal data where it is appropriate to do so."

[5] 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.

18. The ICO has helpfully provided further clarity specifically to HEIs in the case of an emergency. In a blog post on 14 September 2021, making reference to the Code of Practice (which at that time was not in force) it was stated that:

    "Put simply, university and college staff should do whatever is necessary and proportionate to protect someone's life. Data protection law allows organisations to share personal data in an urgent or emergency situation, including to help them prevent loss of life or serious physical, emotional or mental harm."

19. It is clear therefore, that in situations of emergency, HEIs may disclose personal data regarding their student body.

20. The Code of Practice offers practical guidance to planning ahead for data sharing in an emergency or urgent situation to help ensure decisions are made efficiently and in a lawful manner:

    a. Make sure you have undertaken a Data Protection Impact Assessment in respect of the specific scenario of data sharing in an emergency scenario. Consider what types of data are held about the student population and the specifics of that personal data that might need to be disclosed in a crisis. How would the disclosure be carried out to ensure the data is shared in a secure manner?

    b. Plan how you will record the decisions that were taken, the data that was shared and the rationale, to ensure that you don't fall foul of your accountability duty.

    c. Determine who the individuals who will be involved in making key decisions are in advance and ensure that they have had up to date training.

    d. Ensure that appropriate Data Sharing Agreements are in place where there is a need to share data between organisations on a more frequent basis. A good Data Sharing Agreement will set out the purpose of sharing data between the organisations, state what happens to the shared data at each stage of the sharing process, outline the roles and responsibilities of the organisations for the sharing of data and confirms the liabilities of each organisation should something go wrong.

26 October 2021

Matthew Wyard

Barrister
3PB

0117 928 1520
matthew.wyard@3pb.co.uk

3pb.co.uk