FOR LEADERS, FOR LEARNERS

ADVICE & GUIDANCE

Data and its use in schools

Introduction

Schools collect, process, store, use and dispose of different types of data: educational records, personal data and sensitive personal data. This advice document focuses on the latter two categories and the changes to the handling of such data that are scheduled to come into force on 25 May 2018 – the **General Data Protection Regulation** which will effectively replace the current legislative framework, currently enshrined in the **Data Protection Act 1998**.

Personal data, held by schools, is governed by the **Data Protection Act 1998**. To comply with the act, schools must observe the eight 'data protection principles', ensuring that information is:

- used fairly and lawfully;
- used for limited, specifically stated purposes;
- used in a way that is adequate, relevant and not excessive;
- accurate;
- kept for no longer than is absolutely necessary;
- handled according to people's data protection rights;
- kept safe and secure;
- not transferred outside the European Economic Area without adequate protection.

Personal data is information that relates to an identifiable living individual that is processed as data. Processing amounts to collecting, using, disclosing, retaining or disposing of information. The data protection principles apply to all information held electronically or in structured paper files.

The principles also extend to educational records – the names of staff and pupils, dates of birth, addresses, national insurance numbers, school marks, medical information, exam results, SEN assessments and staff development reviews.

Sensitive personal data is information that relates to race and ethnicity, political opinions, religious beliefs, membership of trade unions, physical and mental health, sexuality and criminal offences. Sensitive personal data is given greater legal protection as individuals would expect certain information to be treated as private or confidential – for example, a head teacher may have a school e-mail account that is made publicly available on the school's website whereas their home e-mail account is private and confidential and should only be available to those to whom consent had been granted.

The Data Protection Act requires schools to strike the right balance in processing personal information so that an individual's privacy is protected. Applying the principles to all information held by schools will typically achieve this balance and help them to comply with the legislation. Schools must notify the ICO (Information Commissioner's Office) that they are processing personal data. Schools should ideally nominate an individual (typically, the School Business Manager) as 'Data Controller'. If the principal role and responsibilities for information is not designated, the school will be the Data Controller (or rather the governing body or equivalent) as the appropriate 'body corporate'.

Achieving good practice

This next section sets out what schools should be doing in any event to ensure that their data management and handling practices are at least good and that their houses are in order.

Fair processing - schools should tell parents and pupils what personal information they are collecting and why. Typically, schools should provide what is referred to as a 'Privacy Notice' to parents and pupils, before, or as soon as practicably possible after, you obtain their personal information. There is no prescription for such a notice but there will be examples provided on the ICO website – www.ico.org.uk.

It is also prudent to include the use of CCTV and school photographs of staff and pupils in the privacy notice – these amount to processing personal data as individuals may be identified from the use of such images.

Additionally, access to personal information should ideally be restricted to those who need it to do their jobs. Access controls should be reviewed at appropriate intervals to ensure effective information governance.

Information security

This area of activity is critical – the loss of or unauthorised access to personal information is likely to cause the most harm to a school's reputation, to staff, to parents and pupils and is the most likely action to cause interest from the ICO! If, as a result of a breach of data protection principles, an individual suffers a loss, they have the right to take action for compensation and the ICO has the power to impose significant financial penalties on schools.

Data Controllers should ensure that data is physically secure (e.g. lockable cupboards) and access to information held in hard copy is only accessible by those with a need to use it to do their job. IT systems that back-up personal information should also be reviewed to ensure that these arrangements are also effective. Portable devices (e.g. laptops, memory sticks) that hold personal information should also be subject to review. If hard copies of data need to be taken from their secure home, these can simply be booked out to the relevant member of staff.

The use and review of encrypted passwords can be particularly effective in securing access to electronically-held personal information. Any failure to use adequate software to safeguard personal information will invoke action from the ICO.

School information is often transferred to and stored on privately owned portable devices. In the event that something goes wrong, the school will be responsible for any breach, unless it can prove that it did everything reasonably possible to keep the information secure.

Disposal

The Data Controller is responsible for the disposal of all information held by the school.

Hard copy data should be shredded; soft-copy data should be cleared from the files and memory of devices and IT support colleagues should confirm that records have been cleared.

Policies

Schools ought to have a straightforward policy on Information Management and Governance, sometimes referred to as the acronym IMAGE.

The roles and responsibilities can be set out in such a policy – the ICO love a good policy!

A well-thought-out policy helps to set out standards for record keeping, general practice and will also help to raise staff awareness and underpin any further and ongoing staff development.

Data Protection is generally considered to be a good topic for an INSET day session.

Subject Access Requests (SARs)

Data protection legislation entitles an individual the right to request the personal information a school holds on their behalf – this is known as a Subject Access Request and includes all and any information held by the school, not just that information held on central files or electronically, so it could also include correspondence or notes held by others in the school.

SARs must be responded to within 40 calendar days of receipt. The SAR should be made in writing by the individual making the request. The school may charge a fee for dealing with this request, typically £10. Parents can make SARs on behalf of their children if the children are deemed to be too young or they have consented to their parents doing so on their behalf.

Information that may include the personal information of another individual may need to be redacted especially if the individual is identifiable. In addition, SARs are distinct from the right of access to educational records (under the Pupil Information Regulations) which give a parent a right to information in their children's education record.

Sharing personal information

Schools inevitably share personal information with other organisations such as local authorities, other schools and social services.

When sharing data or considering sharing data, schools must ensure that:

- they have the consent and authority to share information;
- adequate security arrangements are in place to protect the shared information;
- those to whom the data is provided are clearly identifiable.

Websites

Schools are required to have a website and to include certain information on their website.

Websites will also include personal information so it is very important for schools to ensure that:

- personal information (e.g. photos, images) are not used or disclosed without the relevant individual/s being aware; a simple consent form will suffice;
- certain parts of the website are only made available to those that need access to do their jobs (e.g. staff, governors).

CCTV

Many schools will install CCTV for security purposes or to maintain good order in the school.

If you have installed CCTV in your school or are thinking about it, please bear in mind:

- capturing and/or recording images of identifiable individuals amounts to processing personal information and it therefore needs to be in step with data protection principles;
- staff, parents and pupils are entitled to know that you have installed CCTV or are considering it and the reasons why;
- Cameras should only be sited where they are needed for their stated purpose and not where people would be entitled to privacy (e.g. cameras may be installed in school toilets / washrooms but not near urinals or toilets cubicles where privacy would be expected);
- Finally, decide on how long you may wish to keep recorded material and remember that CCTV images can be requested as part of a SAR (we'd recommend that records are wiped after 4 months on the grounds that many employment procedures are time-bound to 3 months).

Photographs

Schools may take photos for publication without specific consent as long as they have indicated their intentions. Care needs to be taken especially where schools publish photos of young pupils, name individuals, put photos on the website or record the school play for selling to parents.

It's always best to be belt and braces and get the consent of those individuals (or their parents) who are more likely to be affected.

Processing by others (e.g. payroll providers)

Under data protection legislation, a third party organisation that processes personal information on the school's behalf is known as a 'Data Processor'. The school (the 'data controller') remains responsible for any processing that a data processor might do for it.

The best and only way to ensure that processing arrangements are adequate is to have an agreement between the school and the data processor that sets out how personal information will be securely processed and the remedies available in the event of a breach of the agreement.

Training

Raising awareness of the role and importance of (management) information among staff, governors, volunteers, parents and pupils will always be welcome.

Using INSET days is ideal for bitesize training sessions for staff in particular.

Freedom of Information (FOI) Act 2000

Under this legislation, all maintained schools and academies should have what's known as a 'publication scheme' – this will help to respond to FOI requests.

A 'publication scheme' typically sets out the kinds of information that the ICO would expect schools to provide. As a minimum, the ICO expect schools to make available information that is required by statute or by the DfE or by virtue of a funding agreement.

Examples of 'publication schemes' for schools in England, in Wales and in Northern Ireland are available (by country) on the ICO website – typically, your employing body (i.e. local authority or academy trust) will usually respond to a FOI request but may need to work closely with schools to validate their response and any disclosed information.

A model publication scheme has been prepared and approved by the ICO; it may be adopted, without modification, by any public body. The model scheme commits the public body to make information available to the public as part of its normal business activities. Further details of the model scheme are available at www.ico.org.uk

How the FOI response is provided and whether any charges are levies will be a matter for discussion and agreement with the requester.

Coming soon!

There are changes ahead! This is the new (and developing) **General Data Protection Regulation (GDPR)**. This change will effectively amount to a new data protection legal framework across the EU. The government has confirmed that its decision to leave the EU will not affect the commencement of the GDPR which is scheduled to come into force on 25 May 2018.

The full extent of the GDPR is still developing – the EU's 'Article 29 Working Party' includes representatives of the data protection authorities from each EU member state. The Information Commissioner's Office is the UK's representative and is committed to helping schools to prepare to meet the requirements of the GDPR ahead of its scheduled implementation on 25 May 2018.

The GDPR applies to both 'data controllers' (e.g. a school) and to 'data processors' (e.g. an external payroll provider). Under the GDPR, new and specific legal obligations will be placed on 'data processors' relating to the maintenance of personal data records and to processing activities, breaches of which will invoke greater liability than before. As a 'data controller' (e.g. a School Business Manager), the GDPR will place greater obligations on you to ensure your contractual agreements with 'data processors' comply with new GDPR guidelines.

The GDPR applies to processing carried out by organisations operating within the EU but also applies to organisations outside the EU that offer goods or services to buyers in the EU.

What information does the GDPR apply to?

The GDPR applies to 'personal data'. However, the definition of 'personal data' will be expanded to include such items as an *IP address* that will be classified as 'personal data'. This particular change, for example, simply reflects the developing and digital technologies, the developing methodologies of data collection and the internationalisation of commercial transactions and general trading arrangements.

Will there be any immediate impact on schools?

The change to the wider definition of 'personal data' will have little immediate impact on schools. Information that falls within the scope of current data protection legislation will also fall within the scope of the GDPR. This said, the advent of the GDPR is a 'wake up' call for all organisations, including schools. The last section of this paper sets out what schools should now be seriously considering and what action/s they should be taking to 'get their houses in order'.

Personal data and Sensitive personal data

All 'personal data', whether held manually or electronically, will fall within the scope of the new GDPR.

The GDPR refers to 'sensitive personal data' as "special categories of personal data" – new categories will include 'genetic data' and 'biometric data' where such data is processed to uniquely identify an individual (e.g. fingerprints, face-recognition, eye-screening).

Principles

The new principles under the GDPR are similar to those under current data protection legislation with added detail at certain points and a new **accountability** requirement. In practice, this means that the GDPR will require schools to show **how** they have complied with the principles – e.g. by documenting the decisions that have been taken about a particular processing activity.

Article 5 of the GDPR requires that '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 of damage, using appropriate technical or organisational measures.

Article 5 (2) requires that "the controller shall be responsible for, and able to demonstrate, compliance with the principles".

This means that the school or the person to whom the overall management of information has been delegated (typically, the School Business Manager), is now, not only responsible for the management of information but they must have systems and practices in place to underpin compliance to the revised 'personal data' principles.

In the next and last section of this paper, we set out what action/s schools should now be seriously considering that will help set the bar at an appropriate level to not only comply with the revised 'personal data' principles but that will, at the same time, demonstrate how compliance has been or will be achieved.

Next steps for schools

Using the advent of the new legislative framework, the **General Data Protection Regulation**, will be the catalyst for measured change for schools that need to get their houses in order.

The case for change is compelling. The new arrangements for handling 'personal data', enshrined in the GDPR, have been brought about by changes in technology, changes in how data is collected, stored and utilised (e.g. genetic data, biometric data), the exposure to identity and other types of fraud, the growing mobility of labour, employment and working arrangements across EU states (and the rest of the world), globalisation and digitalisation and the need to bring data protection legislation, that is approaching its 20th anniversary, a fresh (post-Google) coat of paint! Ironic then that the UK is leaving the EU but this won't affect the development and eventual implementation of the GDPR in 2018.

So, whilst the new arrangements won't commence until May 2018, now is the time to get the GDPR on agendas, sharpen appetites, generate some interest and agree on what needs to be done. The risk for many schools is that they simply don't know whether where they are complying with current data protection legislation. The advent of the GDPR will only exacerbate any uncertainty.

If you're not entirely sure about your school's current 'data' status or your readiness for change, ask yourself this question:

"Can I say, with absolute certainty, and then prove, that the only people who need access to sensitive personal data, can access it?"

If you can't answer 'yes' to this question, you are not protecting personal data and you will therefore (probably) not be aware of any data security breaches. At the very least, it would be prudent to satisfy yourself that 'personal sensitive data' is protected by password/s, that access controls are in place for electronically-held data, or, if data is held in hard copy only, it is secure, especially when it is left unattended.

Another question to consider and to get the 'data' debate underway is:

"Is our school ready to handle a Subject Access Request (referred to earlier in this advice document)?" Additionally, who would deal with such a request? Is there a straightforward process in place to ensure that such requests are handled effectively?

Under the new GDPR framework, the ICO will have a clearer picture of data protection practices and will have the power to impose fines on those organisations that are in breach of the revised data protection arrangements. Claiming to be 'on the case' or 'playing catch-up' will not be a sufficient reason for avoiding a penalty.

To frame any debate, it's really helpful to regard data as a 'critical resource' to the school that needs careful management – data persuades, data underpins important decisions about what to do and what not to do, data helps to shape a school's strategic direction and the individuals needed to achieve it.

If you need a place to begin, it's advisable to start the whole programme with an audit of your school's data, to establish your current position and your departure point. You may even wish to collaborate with neighbouring schools to spread the work and cost of such an exercise. It would be advisable to consult your employing body to establish whether there is any funding available to complete such an audit and any ongoing compliance work.

The aim of any audit will be to get a clear picture of all the types of personal data and sensitive personal data that your school holds and where and how it is stored. You can then begin to design, develop and implement a data protection system that is right for your school. Further monitoring and evaluation will inevitably need to be considered.

To ensure that you remain connected to ongoing developments that relate to the launch of the new data protection arrangements, schools might like to subscribe to the ICO e-Newsletter, a facility available on the ICO website.

If you would like to discuss anything further in this document or would simply like some advice or guidance, then please give us a call on our **NAHT Advice Line on 0300 30 30 333 (option 1)** where we will be very pleased to make arrangements to discuss your situation further.

Alternatively, you can e-mail us at specialistadvice@naht.org.uk and we will promptly respond to you.