May 2024
Management Circular No 53

To: Heads of All Educational Establishments

Management Circular 53 – Data Protection Guidance

1. Introduction

Schools and Education officers at Glasgow City Council process personal data every day. In the collection, storage and processing of personal information regarding pupils, the school is acting as 'data controller'.

This means that the school must satisfy certain obligations in order to comply with the Data Protection Act 2018 (DPA 2018) and the UK General Data Protection Regulation (UK GDPR).

Data protection legislation provides a governance framework through which personal data can be collected and used fairly and lawfully.

2. Definitions

Personal data means, 'any information relating to an identified or identifiable natural person ("data subject"); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

Basically, if a person can be identified from the data, or if the data is a unique reference or identifier of one person, then it will likely fall into the definition of personal data. Examples will include (but are not limited to) names, addresses, email addresses, dates of birth, pupil numbers (for example SEEMIS Reference Number or Scottish Candidate Number)

Special Category Data is personal data which is considered more sensitive than normal personal data and deserving of extra protection. It includes 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.

Processing refers to 'doing something' with personal data which might include collecting, storing, sharing and deleting it.

The Data Protection Principles

The Data Protection Principles require that:

- Personal data is processed lawfully, fairly and in a transparent manner
- Personal data is collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes
- Personal data is adequate, relevant, and limited to what is necessary
- Personal data is accurate and, where necessary, kept up to date
- Personal data must be kept for no longer than is necessary

- Personal data must be processed in a manner that ensures the appropriate security

i. Processing personal data lawfully

Schools will process personal data for a variety of reasons. The reason for doing something with personal data (the purpose) will determine the lawful basis which allows you to do what you want to do.

The lawful basis is also known as a 'condition of processing' under Data Protection legislation. The main conditions of processing, with some examples, are given below.

- **the performance of a public task carried out in the public interest or as part of the Council's official authority**

This will apply to the majority of personal data which schools need to do to deliver education in the local authority. This 'public task' here relates to the Education (Scotland) Act 1980 which provides a general statutory data to provide education but does not dictate specifically how that is to be achieved.

Teachers, practitioners and support staff collect and use personal data a part of carrying out their roles with the reason being to fulfil their duty to deliver education. They are completing the Council's public task. Examples will include collecting data for the school, managing pupil records and collecting Government statistics. These functions will be related to use of a public task.

If a school is introducing a new function or process such as introducing a new educational app then a Data Protection Impact Assessment (DPIA) should be being carried out. More advice on this can be found here.

- **it is necessary as part of a legal obligation, or contract**

This condition will apply when legislation, or a contractual term, specifically directs that personal data must be dealt with in a certain way.

An example of a legal obligation would be when the Council receives a court order.

A contractual obligation might apply if the school or the Council has signed a contract requiring personal data to be collected or shared in a particular way.

- **it is necessary to protect somebody's vital interests**

The condition of processing will apply when you need to share personal data in 'life or death' situations. In practice, this means for the purpose of child or adult protection.

This condition will apply to both cases where you know that there is a child/adult protection concern, and where you need to share personal data in order to establish whether there is.

- **the data subject, or their parent/guardian, has given consent for their personal data being used in that way**

Consent should not be used in any cases where there is no practical alternative to processing personal data in a particular way, or where there can be considered to be an unfair balance of power between the data subject and the controller. In these cases, a different condition of processing is likely to apply.

Think carefully before deciding to use consent as a condition of processing under data protection because. Where consent is to be used as a condition of processing, it needs to be explicit and evidenced, it must also be given by affirmative action.

Consent cannot be assumed through a lack of action, so it is not acceptable to automatically assume that consent exists unless someone tells you otherwise. If you do use consent, you must also be aware that individuals can withdraw their consent at any time and you will need to make it easy for them to do so, you may also need to deleted their personal data if they ask you to.

If consent is to be used, children aged 12 and over will normally be considered mature enough to be able to consent to their data being processed in a particular way. Where a child is under 12, consent should be sought from their parent/guardian.

An example of appropriate use of consent would be pupil photographs that are published beyond school interests such as newspapers, school websites or social media.

ii. Telling people what you do with their data

It is important that people understand why a school collects personal data and what they will do with it. This manages expectations and builds trust by ensuring that people are not surprised by what happens to their data. Data Protection legislation requires us to tell people what we will do with their personal data through a Privacy Notice.

A Privacy Notice could be a leaflet, a web page or a statement on a form. The Council has more information here on Education Privacy Notices. As schools will be processing the personal data of children, privacy information should be expresses in language that children will understand.

iii.Collecting personal data

When collecting or using (including sharing) personal data, it is important to only use what is necessary for the purpose. Always evaluate what information is relevant, proportionate, necessary and do not collect/use more than you need.

If some personal data is essential, and other information is helpful but not essential, the difference should be made clear to the data subject so they can decide how much information they are comfortable providing. This can be included in a Privacy Notice.

iv. Keeping it accurate

Data Protection law requires organisations to have reasonable measures in place to ensure that the personal data they use is accurate and up to date, particularly when the information will be held for a period of time over which it might change.

It is important that inaccurate data is updated when it is known to be wrong. Schools should ensure that they are able to update their records timeously should they be informed that the personal data they hold is no longer correct. Inaccurate data will be any personal data which is factually wrong e.g. incorrect date of birth, change in contact details.

v. How long to keep personal data

Personal data should not be kept for longer than is necessary for the purpose for which it was collected. The Council's Retention and Disposal Schedule sets out the time periods which certain records need to be retained for, and after which they should be disposed. This should be applied consistently to both paper and electronic records.

vi. Keeping personal data secure

Schools need to have reasonable measures in place to protect the personal data they store and use. Security can be managed by adhering to Council policy and local procedures. All staff should have completed relevant training on GOLD which provides general information about responsibilities.

More information can be found here in the Council's Information Security Policy

Protecting personal data can get more complicated if it needs to be shared outside schools. For example, if personal data needs to be emailed to another organisation, it is important to consider whether the transmission is secure and what the impact would be on the individual if the personal data was exposed. It is important to consider how personal data can be exchanged electronically and seek guidance if required.

If a school wishes to introduce a new system or app which will use or store personal data, its security must be assessed to ensure that the Council will not breach Data Protection legislation by using it. It is important to understand whether the system is vulnerable to malware and also where the data is going to be stored. Failure to ensure that the personal data is appropriately secure will result in the Council breaking Data Protection law and committing a breach.

Systems/apps which process personal data should be assessed using a Data Protection Impact Assessment (DPIA). This will assess any data protection principles (not just security). Depending on the circumstances, it may be necessary for specific security information to be provided by the suppliers or security assessments to be carried out.

3. What happens if this goes wrong?

Sometimes there are issues with how personal data is handled and personal data ends up somewhere that it should not. This is known as a Data Breach and may include the following:

- personal data being lost, stolen or accessed in a way it should not have been. This might be through the loss of hardware or paperwork containing personal data
- emails sent to multiple people showing their private email addresses
- disclosure of personal data in error (e.g. a letter or email sent to the wrong person or personal data given over the phone to someone who should not receive it)

The Council's Data Breach Procedures should be followed - more information here . It is essential that you report a potential Data Protection breach as soon as you become aware of the breach. Notifiable breaches should be reported to the ICO within 72 hours.

4. Individual Rights

Individuals have certain rights under data protection law, these include the right to ask what information is held about them, to ask for their personal data to be rectified if it is inaccurate, or, in certain circumstances, not to be processed further or deleted. The main rights which manifest in a school environment are:

- Right to access personal data
- Right to rectify personal data
- Right to erasure, also known as the right to be forgotten

If you wish to find out further information on how to handle a request then please consult MC22.

DOUGLAS HUTCHISON
Executive Director of Education