GDPR Factsheet

From 25 May 2018, General Data Protection Regulation (GDPR) comes into force in the UK. The current Data Protection Act 1998 will be abolished.

The Information Commissioner will have the power to impose fines of up to the higher of 20 million Euros or 4% of turnover.

GDPR imposes new requirements for organisations, including schools and colleges

Whilst many GDPR concepts are similar to those set out in the Data Protection Act 1998, there are a number of new elements.

Changes to the legislation state that schools and colleges must:

- **carry out an information audit**. This should establish what personal data is held across the organisation (including data on children, staff, parents, governors, trustees and suppliers), how the data is collected and processed, the data's location, how securely it is held and who it is shared with. Do you need all of this information, and are there duplications?
- **make sure that when consent is required, it meets the more stringent standards**. Consent must be freely given, specific, informed and unambiguous and with a positive opt-in (for example, use of images of children in school publicity will require permission to include, rather than an opt-out form).
- **appoint a Data Protection Officer (DPO)**. As a 'public authority', schools and colleges require a designated DPO to take responsibility for data protection compliance. Consider your organisation's structure to establish where this role sits best. It should be somebody with sufficient expertise and independence.

GDPR: new provisions designed to develop the **protection of children's personal data** and rights for individuals:

1 The **right** of access.

2 The **right** to rectification.

3 The **right** to erasure.

4 The **right** to restrict processing.

5 The **right** to data portability.

6 The **right** to object.

7 **Rights** in automated decision-making and profiling.

Any questions?

ASCL member hotline

0116 299 1122 | hotline@ascl.org.uk

Information Commissioner's Office (ICO)

www.ico.org.uk

For organisations

https://ico.org.uk/for-organisations/

Department for Digital, Culture, Media and Sport

Outcome of consultation responses – August 2017

www.gov.uk/government/consultations/general-data-protection-regulation-call-for-views

- **promptly notify the Information Commissioner of a breach of security of personal data**. Put procedures in place to detect, report and investigate breaches of security in personal data. GDPR requires all organisations to report data breaches to the ICO within 72 hours of identification where it is likely to result in a risk to the rights and freedoms of individuals, for example, damage to reputation, financial loss or discrimination. Where a breach could result in a high risk to the rights and freedoms of individuals, those individuals should be notified directly.
- **comply with subject access requests**. An individual can request a copy of information you hold about them. This should be provided free of charge and within one month of receipt of the request.
- **ensure written contracts are in place with third parties who process personal data on your behalf**. Schools and colleges must also ensure third party suppliers (for example, parent payment platforms) are GDPR-compliant, and that legally-binding contracts with any company processing personal data are in place.
- **make sure privacy notices are written in a way a child will understand**. Review all privacy notices (ie "all privacy information you make available or provide to individuals when you collect information about them" ICO), and amend as necessary to ensure they are appropriate and written in a way pupils can understand. Check guidance and policies are reviewed and updated for staff and parents, and all policies are easily accessible.
- **be able to demonstrate compliance with GDPR**. This should be through technical and organisational measures including data protection policies, staff training, internal audits of processing activities and internal HR policies. Relevant documentation should also be maintained on processing activities, including data minimisation, transparency, and 'pseudonymisation'.

Association of School and College Leaders
130 Regent Road, Leicester LE1 7PG
T: 0116 299 1122 E: info@ascl.org.uk W: ascl.org.uk Tw: @ASCL_UK

January 2018