Preparing for the General Data Protection Regulation (GDPR)

10 Steps For Schools....

schools BROADBAND™
Your Future. Our Technology.

T: 01133 222 333 E: info@schoolsbroadband.co.uk

Introduction

For more information visit:
www.ico.org.uk

The new EU General Data Protection Regulation (GDPR) comes into force in the UK on 25th May 2018.

This regulation will replace the current Data Protection Act 1998 (DPA) and overhaul many existing data protection rules.

In order to prepare for this change it is important that schools read through the steps which have been set out for them and take into account how they are likely to be affected by GDPR.

Schools should refer to the ICO's 12 Steps Checklist as well as the ICO website for more information on the details provided within this booklet.

For more information visit:
www.ico.org.uk

Step 1 - Raise Awareness

- Schools need to know that data protection law is changing
- It's essential that schools become familiar with GDPR in order for the school to make adjustments accordingly in order to be compliant with the new rules
- A plan of action should be put in place by management so that implications caused by GDPR will not negatively impact the school
- It is recommended that schools designate a Data Protection Officer (DPO) who can lead the process and take on the additional responsibilities of managing the new GDPR framework

For more information visit:
www.ico.org.uk

Step 2 - Accountability and Data Governance

- **Privacy Impact Assessments (PIA)** will now need to be carried out when undertaking 'high risk' data processing activities, i.e. where there's a high risk of an individual's right to privacy being violated

- **Pseudonymisation** is a new term which refers to the way personal data is processed. Pseudonomised information is a form of personal data but GDPR promotes usage in certain circumstances in order to enhance privacy

- **Data Protection Audits** relates to how schools should review and document personal data they hold. Unless you know what personal data you hold and how it is being processed, it will be difficult to demonstrate how the school complies with GDPR

For more information visit:
www.ico.org.uk

Step 2 - Accountability and Data Governance Continued...

- **Data Protection Policy Reviews** - GDPR is likely to require schools to review their data protection policies, which are used to explain an individual's legal rights. Due to GDPR amending the rights, schools' policies also have to be amended

- **Appointment of Data Protection Officer** - it is recommended that all schools now formally appoint a DPO in order to manage the extra responsibilities of ensuring the school complies with the new rules

- **Staff Data Protection Training** - staff data protection training is needed in order to keep personal data secure. New starters as well as existing staff should be given regular training sessions to minimise data loss and other potential errors which may occur

schools BROADBAND™
Your Future. Our Technology.

T: 01133 222 333 E: info@schoolsbroadband.co.uk

For more information visit:
www.ico.org.uk

Step 3 - Communicating Data Protection/Privacy Information

- Schools are required to provide certain minimum information to staff, pupils and parents about how their personal data is processed
- Under GDPR the amount of information which must be provided to individuals will increase significantly
- Some of this is mandatory Privacy Notice information, however additional information may be required in specific cases where the school needs to process personal data for further purposes
- Each Data Protection Officer should review your existing Privacy Notices to ensure they comply with GDPR
- Any changes made to policies should remain consistent with Terms and Conditions of the Parent Contract

schools BROADBAND™
Your Future. Our Technology.

The ICO is currently consulting on a new version of its Privacy Notices Code of Practice. The new version will reflect the new requirements of the GDPR.

For more information visit:
www.ico.org.uk

Step 4 – Legal Grounds for Processing Personal Data

- GDPR sets out legal obligations that must be complied with during the processing of personal data
- Under the new GDPR schools will need to know legal grounds for processing personal data and be able to explain it to pupils and parents

  E.g. legal ground for processing pupil images for identification purposes is because it is necessary for the contract, whereas if the images were used for school marketing, consent is likely to be needed

- Individual rights have been modified which means people are now entitled to have their data deleted if requested, for example if consent is the legal basis for processing

schools BROADBAND™
Your Future. Our Technology.

T: 01133 222 333 E: info@schoolsbroadband.co.uk

For more information visit:
www.ico.org.uk

Step 5 - Consent

- Schools should review how they record consent for processing personal data and consider if any changes are required under GDPR
- “Consent” can still be relied on as a legal ground to process personal data, however meeting the new criteria for valid legal consent under GDPR will be more difficult than it has been previously
- Schools need to ensure that they are given clear consent for the different uses of personal data and don't hide consents within broader contracts
- GDPR requires demonstration that consent has been given, schools will need to review systems for recording consent to ensure they have an effective audit trail

For more information visit:
www.ico.org.uk

Step 6 - Indvidual Rights

The legal rights that individuals have under GDPR are very similar to those under the current DPA, however there are several changes which schools need to be aware of.

The new legal rights under the GDPR include:

- **The right of subject access**
- **To have inaccuracies corrected**
- **To have information erased**
- **To prevent direct marketing (marketing directed to specific individuals)**
- **To prevent automated decision-making and profiling**
- **Data portability** - schools must provide requested information electronically and be in a readable format

schools BROADBAND™
Your Future. Our Technology.

T: 01133 222 333 E: info@schoolsbroadband.co.uk

For more information visit:
www.ico.org.uk

Step 7 - Right of Subject Access

GDPR gives individuals the right to ask the school for a copy of their personal data along with any other information about how it's processed. This is commonly known as a Subject Access Request (SAR).

The new rules for handling SARs are set to change and schools will need to update procedures accordingly.

The main changes are:

- Now free in most cases (used to be a £10 charge)
- Excessive requests can now be charged for or refused
- Deadline reduced from 40 calendar days to within one month.
- Additional information to be supplied e.g. the right to have inaccurate data corrected.
- If you want to refuse a SAR, you need to have policies in place to demonstrate why request is refused

For more information visit:
www.ico.org.uk

Step 8 – Personal Data Breaches

- All schools will have to adopt procedures for detecting, reporting and investigating personal data breaches
- GDPR will introduce mandatory breach notifications to the Data Protection Authority (the ICO) and in some cases also to affected individuals
- Schools will still be obligated to have systems in place to detect and investigate all breaches and also maintain an internal breach register
- If the school detects a breach then they must report it to the supervisory authority without delay and not later than 72 hours after becoming aware of it
- Non-compliance can lead to significant administrative fines. Make sure your network security is up to the job.

schools BROADBAND™
Your Future. Our Technology.

T: 01133 222 333 E: info@schoolsbroadband.co.uk

For more information visit:
www.ico.org.uk

Step 9 – Children

- The new GDPR rules introduce some child-specific provisions, which includes legal notices and the legal grounds for processing children's data
- Codes of Conduct may further restrict the way in which personal data can be processed. Schools should carefully consider whether this is likely to affect them and amend their processes in order to comply
- Where information is specifically directed to a child and the legal ground for processing the data is consent, then parental consent will be required for children aged under 16
- The 16 threshold could also be lowered to 13 by a Member State, however under 13s can never themselves consent to processing their personal data in relation to online services, unless it related to counselling services
- The school as the data controller is required to verify consent has been provided on behalf of the child

For more information visit:
www.ico.org.uk

Step 10 - International Data Transfers

- Transfers of personal data outside the European Economic Area (EEA) will continue to be restricted under the new rules of GDPR, with additional improvements
- Schools need to review and map any personal data outside the EEA, highlighting which transfer mechanisms have been put in place in order for them to comply with GDPR
- Previously, schools have sent personal data outsider the EEA through the use of service providers such as Cloud Service Providers, bulk emailing and web hosting
- GDPR will continue to offer existing methods of transferring personal data
- There are exemptions which enable personal data to be transferred under certain circumstances

schools BROADBAND™
Your Future. Our Technology.

T: 01133 222 333 E: info@schoolsbroadband.co.uk

schools BROADBAND™
Your Future. Our Technology.

For more information visit the Information Commissioner's Office (ICO) website: www.ico.org.uk

t: 01133 222 333 e: info@schoolsbroadband.co.uk w: www.schoolsbroadband.co.uk