General Data Protection Regulations

Factsheet for school support staff

General Data Protection Regulations

UNISON
Education & Children's Services

Introduction

The General Data Protection Regulations (GDPR) give individuals more choice and control over how their data is used.

This factsheet is designed to help you feel confident about how you use and protect data as you go about your work.

The regulations bring in stricter duties, which all organisations, including schools, must follow. A school's Ofsted rating could be affected if the correct data protection procedures and policies are not followed.

Failure to comply with legislation could result in heavy fines, therefore compliance with the regulations is essential.

All staff will have a responsibility to ensure that their own activities comply with GDPR.

What you need to know at work

- GDPR covers all processing of personal data. If you are working in a school, it will apply to any personal data that is processed about pupils (such as education records), staff members (such as HR records), or other interested parties such as governors.
- Your school will have someone with designated responsibility for data protection matters, including GDPR. This will commonly be the headteacher. They will be responsible for ensuring that personal data is correctly collected, stored, used and securely destroyed once it is no longer needed.
- Your school will need to have robust procedures to deal with data protection breaches. A data breach is anything leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure or access to personal data. Most breaches are the result of human error. They are rarely malicious. Under GDPR, certain breaches will need to be reported to the Information Commissioner's Office (ICO). Your employer should have a procedure for this.
- You should never disclose any personal data outside of your school's procedures, or use personal data held on others for your own purposes. Doing so is a breach of GDPR and possibly a criminal offence.
- You should take extra care to ensure that any personal data that you use at work is kept secure. This doesn't need to be complicated or expensive, it is just a case of treating other people's data as you would your own. Actions to consider are:
  - Keeping files in locked cabinets.
  - Using a shredder or a confidential waste bin where data is no longer needed.
  - Having a clear desk policy.
  - Locking your computer screen when you are away from your desk.

- Encrypting removable media USBs (memory sticks), CDs etc so that if they are lost the data cannot be accessed.
- Taking care if working in public – people may be able to see your screen.

Your own rights under GDPR

- You have a right to know what information your employer holds on you and how they are processing it.
- You have a right to access any information that your employer holds on you. This includes information regarding grievances or disciplinary action, or information obtained through a monitoring process/system. If you want to access your data, you should make a subject access request to your employer. They will then have one month to provide the information to you.
- You have the right to ask your employer to delete data that it holds on you. If that data is no longer needed, then your employer should delete it. This is especially useful if a disciplinary matter is put on your record for a specified time – once that time has elapsed it should be deleted and you can ask to ensure it is.

Children's data under GDPR

- The GDPR includes special protections in relation to children's data. This is mostly focused on allowing children to make informed decisions as to how their data will be processed, for example when they are using social media.
- Children have the same rights under the GDPR as adults. This includes the right to make a subject access request.
- Compliance with data protection regulation, including GDPR, should be central to all processing of children's personal data.

When things go wrong…

Data breaches are nearly always the result of human error. The most common data breaches are:

- Paper files or USB sticks are lost.
- An email containing personal data is sent to the wrong person in error. Sometimes the incorrect recipient will have the same name as the intended recipient.
- An email is sent to a group of people using the CC field rather than the BCC field, therefore disclosing everyone's email address to everyone else.
- Personal data is left on desks unsecured.
- An incorrect document containing personal data is attached to an email in error.

…don’t panic!

If you have made an error like those above, don’t panic! You should follow your employer’s breach reporting procedure immediately. If they do not have a breach reporting procedure, tell your line manager about the breach instead. Delaying reporting the incident will only make matters worse.

Once you have reported the breach, you can also contact your UNISON branch for advice.

Further questions

If you have concerns that your employer has misused information, or has not kept it secure and safe enough, you can contact your UNISON branch for advice.

If you work in a school and want expert, professional help on issues like data protection join UNISON.

Not in UNISON?

Join today at **joinunison.org** or call **0800 171 2193** or ask your UNISON rep for an application form.

Published and printed by UNISON, UNISON Centre, 130 Euston Road, London NW1 2AY.
CU/April 2018/24996/3925/UNP 15095.