integra.
your community

Your responsibility:

The Principles of Good Data Handling

Personal data shall be:

- Processed lawfully, fairly and in a transparent way in relation to individuals
- Collected for specific, explicit, and authentic purposes
- Adequate, relevant, and limited to what is needed
- Accurate and kept up to date
- Retained only for as long as necessary
- Processed in a way to maintain security.

What should I do now?

✓ Make sure you know what data you have and use and that it is stored securely

✓ Read the school policies on Data Protection

Good Practice Tips

- Information must be relevant, professionally written and complete. Recorded opinions and intentions are personal data.
- Ensure that all paper records containing personal data are kept securely. Dispose of paper records in confidential waste bins or by shredding.
- Follow the Data Protection and Acceptable Use Policies—copies are available on the school website or from the school office.
- Do not divulge your passwords to anyone else. This includes colleagues even if they seem to have a good reason for having this.
- Follow your school's agreed file retention policies and adopt a clear desk approach. Do not make additional copies and save them on other drives.
- Never share personal data without a proper reason
- Always lock your computer when you are away from your desk (windows + L)

General Data Protection Regulation

An overview

Copyright Integra 2018 | All Rights Reserved

What is the General Data Protection Regulation?

The GDPR replaces the Data Protection Act 1998. The Regulation becomes enforceable from 25 May 2018.

The GDPR contains new provisions intended to enhance the protection of everyone's personal data and with it, increased fines of up to €20M for failing to do so.

It's all about personal data and privacy.

Individuals Rights

The right to be informed
The right of access
The right to rectification
The right to erasure
The right to restrict processing
The right to data portability
The right to object
The right not to be subject to automated decision making and profiling

Definitions

? **Personal Data** is data that relates to a living individual who can be identified from that data. For example: name, or address, or date of birth, a photograph or bank details, or an IP address. It could be in a computer system or on paper.

? **Sensitive Personal Data** is a special category that requires additional protection, and includes: health, race/ethnicity, sexual life/orientation, political and religious views, trade union membership, genetic and biometric data.

? **Data Subject** is an individual who is the subject of personal data.

? **Processing** refers to anything a school does with personal data – collecting, using, analysing, sharing, storing and disposal.

Keep data safe and do not disclose it to anyone outside of school, only use it for what you have been given it for and don't keep it longer than is needed.

What is a data breach?

A data breach is any situation where an outside entity gains access to user data without permission of the individual, the loss of the data or even the loss of access to the data.

If a data breach should occur, the GDPR specifies that organisations must provide adequate notification. The school has 72 hours to notify the ICO and must inform individuals if their data is affected. The school has policies and procedures in place to deal with this once a breach is noticed.

Report any security incident immediately to your headteacher or a senior member of staff. If it is a breach the school has 72 hours to report it to the ICO.

Copyright Integra 2018 | All Rights Reserved