St Michael's C.E (Aided) Primary School

Data Protection Briefing for School Staff

Data Protection Briefing for School Staff

What's new?

From 25 May 2018, the General Data Protection Regulation (GDPR) became enforceable in the UK. There is also a new Data Protection Act 2018. Much of what you already do will remain in place as these new laws build on what is already law.

The new law requires schools to have a Data Protection Officer. The Data Protection Officer for St Michael's C.E Primary School, is Matthew Keeffe from RADCaT Ltd.

The new law also requires serious data breaches to be reported to the national regulator, the Information Commissioner's Office (ICO). If you discover that any personal data has been lost or disclosed in error, you must report it immediately as per your data protection policy.

What are the data protection principles you must follow?

These are the main principles. Personal data must be:

- used fairly and lawfully
- used for limited, specifically stated purposes
- used in a way that is adequate, relevant and not excessive
- accurate
- kept for no longer than is absolutely necessary
- kept safe and secure

What are data subject rights?

Individuals have various rights under the data protection legislation. They can ask for a copy of the data you hold on them or complain about how you've used the data. You need to be able to spot such requests from parents, pupils and staff and log them with the Data Protection Officer who will respond to them. The rights are:

- **The right to be informed:** about who you are, what data you need and why, and what you will do with it – this is all about being transparent and will be covered in the school's privacy notice
- **The right of access**: to receive a copy of their own personal data and supplementary information
- **The right to rectification**: to have inaccurate personal data rectified or completed if it is incomplete.
- **The right to erasure:** GDPR introduces a right for individuals to have personal data erased. The right to erasure is also known as 'the right to be forgotten'.
- **The right to restrict processing:** to request the restriction or suppression of their personal data. This is not an absolute right and only applies in certain circumstances.
- **The right to data portability**: allows individuals to obtain and reuse their personal data for their own purposes across different services, and to move, copy or transfer personal data easily from one IT environment to another in a safe and secure way, without hindrance to usability.
- **The right to object:** to processing based on legitimate interests or the performance of a task in the public interest/exercise of official authority (including profiling); direct marketing (including profiling); and processing for purposes of scientific/historical research and statistics

- **Rights in relation to automated decision making and profiling.** You can only do this type of processing in certain circumstances and individuals can ask for human intervention in decision-making

What happens if something goes wrong?

You need to report any incident which compromises the security or personal data to the Data Protection Officer. They will consider what has happened and any action which needs to be taken, including whether the incident is a breach of the data protection legislation and, if so, whether it needs to be notified to the ICO.

The ICO has powers to make the school take action or stop processing personal data in ways which affect the privacy of individuals. Where there are very serious breaches, the ICO has the power to fine the school up to £17million, and your Ofsted rating could be affected.

Individuals may also take a civil claim against the school.

What do I need to do?

Always take a moment to double check any data you send anywhere. Please read the following advice:

Tips for keeping personal data safe:

DO

	Keep all personal data locked away at the end of the day and be careful if you take things home so that family members cannot see what they shouldn't see.
	Use school issued encrypted laptops and USB sticks if available, and securely connect to the school network for remote working if you have access.
	Use Egress or a similar system to send personal data to the Local Authority and minimise the amount of personal data you share to only what is necessary.
	Always double check an email before you send it. Check the 'To address' (autofill may have put the wrong person in!) and always double click and open any attachment to re-check it's the right one.
	Ask for help if you're not sure if you can share data from your Data Protection Officer. Take advice from your Designated Safeguarding Lead (DSL) if it's a safeguarding issue.
	If you move classrooms, make sure no data about any children, parents or staffs are left behind in that room. Check down backs of drawers and radiators.

DON'T

	Don't CC emails to groups of people. Always BC (blind copy) them or set up a group.
	Don't use unencrypted USB sticks to transfer children's data, and don't use personal email (e.g. Gmail, Hotmail).

	Don’t share passwords or write them down where people can find them. Ask IT for alternative solutions.
	Don’t leave pupils’ data in your car unattended.
	Don’t leave your computer logged in if it is unattended for long periods

Please sign once you have read the Data Protection Briefing for School Staff and return to Alison Drayton.

Staff member to sign:

I confirm that I have read this data protection briefing.

Name: _____ Signature: _____ Date: _____