GDPR – DATA BREACHES

CATEGORIES OF DATA BREACH

WHAT IS A PERSONAL DATA BREACH?

A personal data breach means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data. This includes breaches that are the result of both accidental and deliberate causes. It also means that a breach is more than just about losing personal data.

Example;

Personal data breaches can include:

- access by an unauthorised third party;
- deliberate or accidental action (or inaction) by a controller or processor;
- sending personal data to an incorrect recipient;
- computing devices containing personal data being lost or stolen;
- alteration of personal data without permission; and
- loss of availability of personal data.

A personal data breach can be broadly defined as a security incident that has affected the confidentiality, integrity or availability of personal data. In short, there will be a personal data breach whenever any personal data is lost, destroyed, corrupted or disclosed; if someone accesses the data or passes it on without proper authorisation; or if the data is made unavailable, for example, when it has been encrypted by ransomware, or accidentally lost or destroyed.

Recital 87 of the GDPR makes clear that when a security incident takes place, you should quickly establish whether a personal data breach has occurred and, if so, promptly take steps to address it, including telling the ICO if required

Data breaches at any level are to be reported as soon as possible to the data lead within the school via email or completion of the data breach form. The data lead will then decide to contact the DPO. All level 3 category breaches will require the meeting of a crisis team to decide next steps, outcome and impact management

LEVEL 1 – MINOR

Description	Breach	Fix
Personal information left on a desk (or in view), on return the document is still there.	Who could have seen this personal information? Which 3rd parties have had access to this room?	Clear Desk policy to be adhered to. Room to be locked. Documents to be locked away.
Personal information saved on a staff or pupil shared area	Who could have seen this personal information? Who could have copied this information?	All documents containing personal data to be password protected or kept in areas of restricted access.
Not saving documents with the correct year.month format	Document storage becomes difficult to manage and retention policy becomes difficult to adhere to	Use the year.month.document name format.

Not emailing with the correct subject format when email contains personal information.	Has the subject disclosed personal information? Is the email subject appropriate to its content? Can the email be appropriately searched for?	Use the following format, Initials.year group.subject e.g. JS.Y11.Safeguarding

LEVEL 2 – INTERMEDIATE

Description	Breach	Fix
Email communication with in school and outside school containing opinions regarding data subjects.	Email message will be included in a subject information access request. Opinions not required.	All email communication should contain fact alone. Steps should be taken to anonymise any other data subjects, should the email not be about them.
Email sent to the incorrect person.	Personal data sent to incorrect people/companies	Emails to be carefully checked before sending. Email protocol to be followed
Email sent to additional people who do not have a requirement for that information.	Personal data sent to incorrect people/companies	Ensure emails are only sent to required recipients.
Unsecure disposal of personal information	Personal data left exposed for third parties.	Use secure methods of disposal
Personal information left on a photocopier.	Personal data left exposed for third parties.	Remain with copier at all times when printing off personal information
Failure to report a minor breach	Breached protocol not adhered to.	Follow the breach reporting policy

LEVEL 3 – MAJOR

Description	Breach	Fix
Personal data shared with a third party without a risk assessment taking place.	Personal data sent to incorrect people/companies.	DPO informed. Retraining of staff. Size and impact of data breach identified. Possible formal action required.
Personal sensitive data shared with a third party without a risk assessment taking place.	Personal data sent to incorrect people/companies.	DPO informed. Retraining of staff. Size and impact of data breach identified. Possible formal action required.
Personal sensitive data sent to a third party without encryption.	Personal data sent to incorrect people/companies. Data corrupted/exposed.	DPO informed. Retraining of staff. Size and impact of data breach identified. Possible formal action required.
Communication with a Third party regarding a member of the school that has not been authorised.	No authorisation sought. No impact risk assessment on data transfer	DPO informed. Retraining of staff. Size and impact of data breach identified. Possible formal action required.
Books/work lost Data sheets/seating plans lost	Loss of personal data	DPO informed. Retraining of staff. Size and impact of data breach identified.

		Possible formal action required.
Unsecure disposal of personal sensitive information	Personal/sensitive data disclosed	DPO informed. Retraining of staff. Size and impact of data breach identified. Possible formal action required.
Personal sensitive information left on a photocopier.	Personal/sensitive data disclosed	DPO informed. Retraining of staff. Size and impact of data breach identified. Possible formal action required.
Failure to report an intermediate breach.	Breached protocol not adhered to.	DPO informed. Retraining of staff. Size and impact of data breach identified. Possible formal action required.
Loss or theft of a device containing personal data	Personal/sensitive data disclosed/lost	DPO informed. Retraining of staff. Size and impact of data breach identified. Possible formal action required.