Personal Data Breach Guidance/Information for Schools – (2021)

Definition:

A personal data breach is defined in the UK GDPR as a *"breach of security leading to the accidental or unlawful; destruction, loss, alteration, unauthorised disclosure of, or access to personal data transmitted, stored or otherwise processed."*

Tips – Identifying a Personal Data Breach:

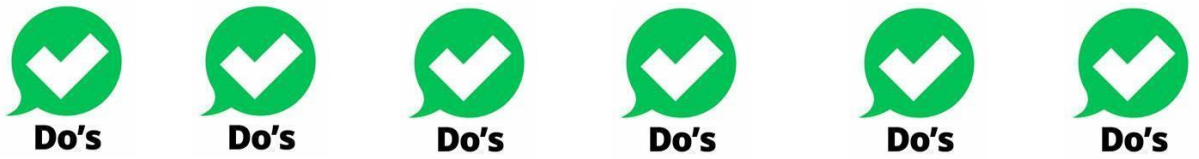
- A personal data breach can include:

  a. Access to information by those not authorised;
  b. Deliberate action by a member of staff or a contractor;
  c. Sending information contained in emails, letters, messages etc. to the wrong address of a person;
  d. Laptops, USB, CDs etc. being lost or stolen;
  e. Alteration or deletion of personal data without authorisation;
  f. Information not being available when required, and this unavailability has a significant negative affect on individuals.
  g. Cyber incidents effecting the personal data contained within computer systems

- If you come across an incident where the **integrity**, **availability** or **confidentiality** of personal data has been affected – you've identified a personal data breach.

Tips - Your Next Steps after Identifying a Personal Data Breach (Do's and Don'ts):

DO  		
Act Quickly!		**DON'T "Deal with it after the weekend."**
DO Inform the Headteacher & DPO!		**DON'T "Leave it for somebody else to deal with"**
DO Investigate!		**DON'T Be afraid of self-reporting.**
DO Document!		**DON'T try to cover up a breach.**
DO Consider reporting to the ICO and informing Data Subjects!		**DON'T Panic!**



1. **DO Act Quickly!**

   - As soon as you're made aware of a personal data breach, try to contain the information immediately by making every reasonable effort: Can you recall an email? Can you contact the incorrect recipient and ask that they delete the information? THINK: What *can I do, within reason to contain this breach? If you're not ICT savvy, don't try to debug a hacked system!*
   - The DPO only has 72 hours to report personal data breaches to the ICO and in some circumstances the incident will need to be fully investigate, especially when the events are not exactly clear.

2. **DO Inform the Headteacher & DPO!**

   - The DPO should be made aware of every single personal data breach from the outset so that they can help you eliminate all risks posed by the breach whilst advising on how best to contain it if you haven't been able to do so.
   - Your DPO can be contacted on information.compliance@powys.gov.uk

3. **DO Investigate!**

   - Channel your inner Sherlock Holmes - you need to find out:

- what has happened?
- how it happened?
- why it happened?
- how many data subjects have been affected?

- You need to document this information in case the ICO requests to see it.
- When you carry out an investigation, ask to see proof – email trails, user logs, document histories etc. Sometimes people don't give you the full story behind a personal data breach, so don't be afraid to question them or request more information including proof if it doesn't add up.

4. **DO Document!**

- If a serious breach has been reported to the ICO who have asked to see your investigation, they might request to see other information as well, including
  - Your recording logs
  - Your investigation reports
  - The information connected with the personal data breach

- You must make sure you document everything correctly in a way that would allow you to pull everything quickly and easily from where it is kept if requested by the ICO.
- Holding good records will also help you improve how you handle personal data breaches

5. **DO Consider Reporting to the ICO**

- The DPO will discuss with you in order to make this determination.
  - The ICO's reporting template can be found on their website (www.ICO.co.uk) and following their form helps you to think about all relevant details surrounding the personal data breach.
  - The DPO will then, if required, report to the ICO.

6. **DON'T "deal with it after the weekend."**

- It's easy to want to leave anything until Monday morning after a hard week, but the ICO's 72-hour deadline for reporting personal data breaches doesn't stop over the weekend or during any bank holidays (including Christmas!). If you have identified a personal data breach at 4.10pm on a Thursday afternoon, then the DPO has until 4.10p.m. Sunday afternoon for it to be reported.
- The first 24/48 hours are vital when you are pulling an investigation report together. Discuss with all involved and try to ascertain the details you need. Leaving it until the last minute to investigate might mean you miss the opportunity to speak to someone and therefore important details may get missed.

7. **DON'T "leave it for somebody else to deal with"**

    - Everyone in the School is responsible for the appropriate processing of personal data, including taking responsibility of a personal data breach when you come across or cause one.
    - Don't think that because someone is more or less senior than you that they will take the breach off your hands.

8. **DON'T be afraid of self-reporting.**

    - Everyone makes mistakes but it's more important to admit to those mistakes when you have caused a personal data breach.
    - Informing the right people immediately could prevent the information from being inappropriately disclosed further – preventing any further risks to individuals.

9. **DON'T try to cover up a breach.**

    - Whether it is yourself or a colleague who is responsible for causing a personal data breach, you need to make sure it is reported correctly and quickly.
    - Don't try to cover it up as doing so could result in the information being used in a way that results in significant harm to an individual if left unmanaged.

10. **DON'T Panic!**

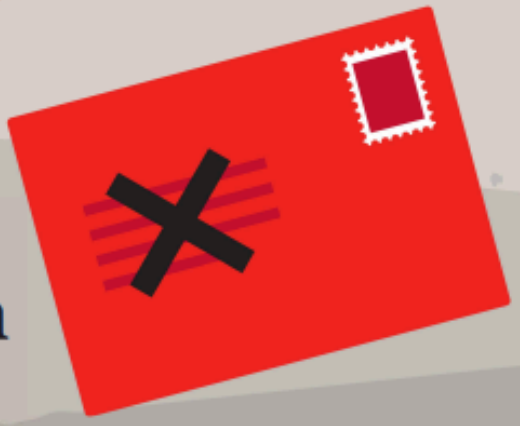
    - It's important to stay calm when you deal with personal data breaches. Remain calm, and try to remember these key points:
        - Contain the breach of personal data immediately (if you can);
        - Make the DPO aware of the breach;
        - Investigate the breach;
        - Where requested, help the DPO report the breach to the ICO (if appropriate) and within 72 hours (this means providing information when requested by the DPO);
        - Mitigate further occurrences of similar breaches.

There are some useful posters below that have been produced by the ICO which you can circulate to all staff:

What does the ICO say?

Common types of breaches

Personal data sent to the wrong person



Unauthorised access to personal data

Loss or theft of personal data

ico.
Information Commissioner's Office

Tips to avoid loss or theft of personal data

- Understand what personal data you have and where it is stored.
- Check the security of the storage is appropriate to the sensitivity of the information.
- Have a clear policy about taking personal data off site and ensure staff adhere to it.
- Ensure adequate security is applied to devices, such as encryption or two-step verification.

ico.
Information Commissioner's Office

Tips to avoid unauthorised access to personal data

- Ensure access is limited to only those who need to have it.
- Have a confidentiality policy and ensure staff are aware of the implications of breaching it.
- Save files to restricted areas where necessary.
- Don't share passwords.

ico.
Information Commissioner's Office

Tips to avoid sending personal data to the wrong person

- Disable the autocomplete function in email services.
- Check record management systems have the most up to date information.
- Ensure mechanisms are in place to double check addresses before sending any personal data.
- Ensure staff are trained and understand the implications of sending personal data to the wrong person.

ico.
Information Commissioner's Office