Personal Data Breaches

What is a personal data breach?

A personal data breach is any incident involving the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data. A breach therefore occurs whenever personal data is lost, stolen, destroyed, damaged or disclosed and where the confidentiality, integrity or availability of personal data has been affected.

“Destruction” includes data that no longer exists or no longer exists in a form that is of any use to the school / academy trust. “Damage” is where personal data has been altered, corrupted or is no longer complete. “Loss of personal data” includes loss of access to personal data.

A breach can be more than just about losing data. A breach can also be about the disclosure of, or access to data by an unauthorised person or third party.

Examples may include:

- The loss or theft of an electronic device which contains personal data, for example a laptop, USB stick or mobile phone.
- Access to personal data by an unauthorised person or third party, such as allowing a person lawfully visiting the school premises to see personal information about a person which they do not need to see
- Sending personal data to the wrong recipient, whether by post, email, text messaging, telephone calls or other means.
- Alteration of personal data without permission.
- Loss of availability, or destruction or damage of personal data
- Information stolen via cyber attack
- ‘Blagging’ or ‘phishing’ offences – where information is obtained verbally or electronically by deceiving the organisation which holds it.

What do I do when a data breach occurs?

The school / academy trust's Data Protection Policy should stipulate the procedure for reporting and dealing with a personal data breach. The procedure should be applicable to all members of staff, volunteers etc. at the School/Academy. We recommend that this should reflect the following escalation:

1. As soon as a member of staff/ volunteer etc. discovers or suspects that a data breach has occurred, it must be immediately reported to the school / academy trust's Data Protection Champion / Lead / Contact.
2. The school / academy trust's Data Protection Champion / Lead / Contact should assess whether a breach of personal information has occurred. Breaches should be investigated as to how and why the breach has occurred and the level of severity. This information should be recorded on the Personal Data Security Breach Incident Form (see Appendix 1).

All personal data breaches, including 'internal' personal data breaches (i.e. where personal data has not left the school), should be logged and thoroughly investigated before deciding on what action should be taken. It is important to ensure that steps are taken immediately to contain and mitigate the effects the potential breach may have on any individual. Where relevant, this should include make reasonable efforts to recover and/ or contain any information that has been breached.

All members of staff should receive appropriate training on how to identify a personal data breach and the school's policy for reporting such an incident.

When should I report a personal data breach to the Data Protection Officer (School DPO Service)?

'Internal' personal data breaches, as described above, should be reported to the School DPO Service where it is believed they are 'severe' and therefore it is necessary to report the breach to the Information Commissioners Office (ICO).

If an ‘external’ personal data breach occurs (i.e. where personal data has left the confines of the School/ Academy/) trust community, the incident should be reported to the School DPO Service as Data Protection Officer as soon as possible, and a completed Personal Data Security Breach Incident Form should be submitted.

The School DPO Service will use the information provided on the Personal Data Security Breach Incident Form to assess the situation, the severity of the breach and whether the incident should be reported to the ICO. The School DPO Service may have additional questions for the school / academy trust in relation to the incident, and we would therefore be grateful if responses to queries raised could be communicated to the DPO Service as soon as possible, in order to report the breach to the ICO within the statutory timeframe if appropriate.

For all personal data breach incidents, the School DPO Service will provide advice on any necessary actions that should be taken and make recommendations to the school / academy trust on its policies and/ or procedures to prevent similar incidents occurring in the future. It is the responsibility of the school / academy trust, as the data controller, to implement any recommended actions identified.

To report a breach to the School DPO Service, please complete the Personal Data Security Breach Incident Form and send to schooldpo@warwickshire.gov.uk . Please ensure that the subject line reads ‘PERSONAL DATA BREACH QUERY’ – this will assist the team in sifting these queries and responding in timely manner.

Does the personal data breach need to be reported to the Information Commissioner’s Office (ICO)?

The GDPR makes it incumbent upon the data controller to report certain types of data breaches to the ICO within 72 hours of becoming aware of the breach. Clearly there are circumstances in which this will be very difficult to comply with, but it must always be the aim to avoid the possibility of sanctions relating to this delay.

Personal data breaches must be reported to the ICO where they are deemed to be ‘severe’; this means where the breach is considered likely to result in a risk to an

individual's rights and freedoms. In assessing whether such a risk exists, it is important to focus on the potential negative consequence for the individual who personal data has been breached. This advice note and the School DPO Service will assist you in making this determination.

Guidance suggests that a school / academy trust should be regarded as having become "aware" of a breach when it has a reasonable degree of certainty that an incident has occurred that has led to personal data being compromised.

It is therefore recommended that the school / academy has a procedure in place for the reporting of personal data breaches that occur or are discovered outside of school time (i.e. weekends or in school holidays). This is particularly important for those incidents that will require immediate remedial action to contain the incident or to prevent further misuse of the personal data (e.g. where the affected individual's may need to be notified).

The ICO recognises that it will not be possible to investigate a breach fully within 72 hours. However, where a serious breach has occurred, the initial report to the ICO must be made within that time. Additional information that is uncovered as part of the ongoing investigation can be provided in phases, as long as it is done without undue further delay.

Whilst a decision may be made initially that it is not necessary to report a breach; any new information that comes to light regarding the incident must be provided to the School DPO Service as soon as possible. If for example, the school / academy is made aware that personal data has been further processed and is likely to result in a risk to an individual's rights and freedoms, it may alter the decision as to whether the incident should be reported to the ICO.

What information should be considered when assessing the risk to an individual rights and freedoms?

- The Personal Data Security Breach Incident Form asks specific questions about the personal data breach. The following information should also be considered

and included as part of the form; this will assist the School DPO Service in determining if the breach should be reported to the ICO:What type of data is involved?

- Is the personal data “special category” information (For further information and a definition of the latter, please refer to the School DPO Service Bulletin number 4)?
- If relevant, was the device encrypted?
- What has happened to the data?
- If data has been stolen or accidentally released to the wrong individuals, could it be used for purposes which are harmful to the individuals to whom the data relates?
- Regardless of what has happened to the data, what could the data tell a third party about the individual?
- How many individuals’ personal data has been affected by the breach and who are they? i.e. the age and vulnerabilities of the affected individual(s)
- What harm can come to those individuals? In particular, are there risks to physical safety or reputation, of financial loss or a combination of these and other aspects of their life?
- Are there wider consequences to consider such as a risk to life?
- Is there likely to be a loss of public confidence in the School / Academy Trust as a result of the breach?
- What steps have been taken to mitigate the breach? Has the breach been contained or the personal data recovered?

Failure to report a serious or severe breach to the ICO can result in the school/academy receiving a significant fine. Don’t forget that sensitive data could mean very little to an opportunistic laptop thief while the loss of apparently trivial snippets of information could help a determined fraudster build up a detailed picture of a person.

Is the school/academy trust responsible for personal data breaches by a third party?

As the data controller, the school / academy trust will retain overall responsibility for the protection of its personal data; regardless of whether the breach has been as a

result of the actions of a third party, for example, an organisation with whom you are under a legal duty to share the information with or and external agenciy which processes personal information on your behalf (such as a payroll provider) but without there being a formal written contract being in place. The third party has an important part to play to enable the controller to comply with its obligations, including potential breach notification. Any processing by a third party is required to be governed by a contract or data sharing agreement/data processing agreement and each of these should stipulate that the third party shall assist the school / academy trust in their obligations by reporting a breach to the data controller “without undue delay”. The School DPO Service has provided standard clauses which should be included as part of any existing contracts. The data sharing agreements / data processing agreements we have provided also include these standard clauses and should be implemented with those agencies for which there is no formal contract in place (see bulletins 8, 8.5 and 10 for further advice).

The third party processor is not required to first assess the likelihood of risk arising from a breach before notifying the school / academy trust; it is the responsibility of the school / academy trust to investigate and make this assessment on becoming aware of the breach.

The legal responsibility for notifying the ICO also remains with the school / academy trust.

Should we notify affected individuals of any breach?

If there is a high risk to the rights and freedoms of any individual as a result of the breach, the individual should be notified as soon as possible. However, in the first instance you can contact your School DPO Service who will be able to advise you on this.

Again, we will need to assess both the severity of the potential or actual impact on individuals as a result of a breach and the likelihood of this occurring. If the impact of the breach is more severe, the risk is higher; if the likelihood of the consequences is greater, then again the risk is higher. In such cases, you will need to promptly inform

those affected, particularly if there is a need to mitigate an immediate risk of damage to them. One of the main reasons for informing individuals is to help them take steps to protect themselves from the effects of a breach.

Notwithstanding the above, it may well be appropriate to notify individuals of breaches in other cases even when there is not a high risk. You will need to consider what is appropriate given the relationship of trust that you have with pupils, staff and parents, and we will make recommendations for such notifications when we consider it appropriate.

The following information should be provided to any individual whose personal data has been affected:

- A description of the nature of the breach
- The name and contact details of the data protection officer or other contact point
- A description of the likely consequences of the breach; and
- A description of the measures taken or proposed to be taken by the controller to address the breach, including, where appropriate, measures taken to mitigate it possible adverse effects.

Am I required to document all personal data breaches?

Yes – the school/academy should document all personal data breaches, regardless of whether or they need to be reported to the School DPO Service or the ICO.
The GDPR requires the school / academy trust to document the facts relating to the breach, its effects and any action taken to mitigate the breach or to prevent a recurrence (in relation to the school/academy's policies, procedures or training). All breaches should be investigated with the use of the Personal Data Security Breach Incident Form and recorded on the Personal Data Security Log (Appendix 2).
Both of these documents are for the school's internal use but you will be asked to present these as part of the audit by School DPO Service. In certain circumstances, the ICO may also request to view your records relating to personal data breaches.

Using these documents to record the information will also ensure the school / academy trust are complying with it overall duty with the Accountability principle under GDPR.

A school / academy trust should also retain documentation relating to the reasoning for the decisions taken in response to a personal data breach; particularly where the breach has not been notified, a justification should be documented (reasons why it is considered the breach is unlikely to result in a risk to the rights and freedoms of individuals.

Ensuring you are prepared for a personal data breach - checklist

☐ We know how to recognise a personal data breach.

☐ We understand that a personal data breach isn't only about loss or theft of personal data.

☐ Our staff know how to escalate a security incident to the appropriate person or team in our organisation to determine whether a breach has occurred.