




HIGH WELL SCHOOL
Preparing for Positive Futures

Personal Data Breach Procedure

Policy Lead:	Business Manager
Date approved by Governing Body:	10.05.2022
Date Shared with Staff:	12.05.2022
Date of Review:	May 2023

Signed by Chair of Governors:	
Date:	May 2023

Contents

1. Personal Data Breach Meaning	3
2. Cyber Attacks	3
3. Personal Data Breach Procedure	4
4. Actions to minimise the impact of data breaches	6

1. Personal Data Breach Meaning

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. This may include:

- Sensitive information being disclosed via email (including safeguarding records)
- A school laptop containing non-encrypted sensitive personal data being stolen or hacked
- Hardcopy reports sent to the wrong pupils or families
- Cyber Attack

2. Cyber Attacks

A cyber attack is an assault launched by cybercriminals using one or more computers against a single or multiple computers or networks. A cyber attack can maliciously disable computers, steal data, or use a breached computer as a launch point for other attacks.

The Department for Education and the National Cyber Security Centre (NCSC) has been made aware of an increasing number of cyber-attacks involving ransomware infection affecting the education sector.

It is important that senior leaders in education settings understand the nature of the threat and the potential for ransomware to cause considerable damage to their institutions in terms of lost data and access to critical services.

The Department for Education supports the National Crime Agency's recommendations not to encourage, endorse, or condone the payment of ransom demands. Payment of ransoms has no guarantee of restoring access or services and will likely result in repeat incidents to educational settings.

If a cyber attack happens, High Well School will:

- Enact the School's personal data breach procedure
- Contact the NCSC (National Cyber Security Centre)
- Contact the local law enforcement and Action Fraud (actionfraud.police.uk)
- Inform the DfE by emailing sector.securityenquiries@education.gov.uk

Alamo (High Well School's IT provider) carry out the following to minimise risk:

- run backups every evening, 7 days a week, to take a copy of all the data the school currently holds. They take the backup to a disk, so in the event that the school goes off line due to any type of cyber attack they still have the data physically in school available for a restore should they need to.
- Each week they complete various checks of things "behind the scenes" this includes checking the backup to ensure they are running correctly and make sure there is enough space on the disks.

- They also run Sophos which is a high performance, anti-virus software which is constantly running on every device in search for Virus', Malware, Ransomware etc to try and prevent attacks as much as possible.

3. Personal Data Breach Procedure

This procedure is based on guidance on personal data breaches produced by the Information Commissioner's Office (ICO).

- On finding or causing a breach, or potential breach, the staff member, governor or data processor must immediately notify the Schools Business Manager (Data Protection Officer - DPO) and / or headteacher by email.
- The DPO will investigate the report, and determine whether a breach has occurred. To decide, the DPO will consider whether personal data has been accidentally or unlawfully:
 - Lost
 - Stolen
 - Destroyed
 - Altered
 - Disclosed or made available where it should not have been
 - Made available to un-authorized people
- Staff and governors will cooperate with the investigation (including allowing access to information and responding to questions). The investigation will not be treated as a disciplinary investigation.
- If a breach has occurred or it is considered to be likely that is the case, the DPO will alert the headteacher and the chair of governors.
- The DPO will make all reasonable efforts to contain and minimise the impact of the breach. Relevant staff members or data processors should help the DPO with this where necessary, and the DPO should take external advice when required (e.g. from IT providers). (See the actions relevant to specific data types at the end of this procedure).
- The DPO will assess the potential consequences, based on how serious they are, and how likely they are to happen before and after the implementation of steps to mitigate the consequences.
- The DPO will work out whether the breach must be reported to the ICO and the individuals affected using the ICO's self-assessment tool.
- The DPO will document the decisions (either way), in case it is challenged at a later date by the ICO or an individual affected by the breach. Documented decisions will be stored in the Management area of our school's computer system.
- Where the ICO must be notified, the DPO will do this via the 'report a breach' page of the ICO website, or through its breach report line (0303 123 1113), within 72 hours of the school's awareness of the breach. As required, the DPO will set out:
 - A description of the nature of the personal data breach including, where possible:
 - The categories and approximate number of individuals concerned

- The categories and approximate number of personal data records concerned
- The name and contact details of the DPO
- A description of the likely consequences of the personal data breach
- A description of the measures that have been, or will be taken, to deal with the breach and mitigate any possible adverse effects on the individual(s) concerned
- If all the above details are not yet known, the DPO will report as much as they can within 72 hours of the school's awareness of the breach. The report will explain that there is a delay, the reasons why, and when the DPO expects to have further information. The DPO will submit the remaining information as soon as possible.
- Where the school is required to communicate with individuals whose personal data has been breached, the DPO will tell them in writing. This notification will set out:
 - A description, in clear and plain language, of the nature of the personal data breach
 - The name and contact details of the DPO
 - A description of the likely consequences of the personal data breach
 - A description of the measures that have been, or will be, taken to deal with the data breach and mitigate any possible adverse effects on the individual(s) concerned
- The DPO will consider, in light of the investigation and any engagement with affected individuals, whether to notify any relevant third parties who can help mitigate the loss to individuals – for example, the police, insurers, banks or credit card companies.
- The DPO will document each breach, irrespective of whether it is reported to the ICO. For each breach, this record will include the:
 - Facts and cause
 - Effects
 - Action taken to contain it and ensure it does not happen again (such as establishing more robust processes or providing further training for individuals)

Records of all breaches will be stored in the Management area on our School's computer system.

- The DPO and headteacher will meet to review what happened and how it can be stopped from happening again. This meeting will happen as soon as reasonably possible.
- The DPO and headteacher will meet regularly (bi-weekly) and will assess any recorded data breaches and identify any trends or patterns requiring action by the school to reduce risks of future breaches.

4. Actions to minimise the Impact of data breaches

Below are the steps that High Well School will try to take to try and mitigate the impact of different types of data breach if they were to occur, focusing especially on breaches involving particularly risky or sensitive information. We will review the effectiveness of these actions and amend them as necessary after any data breach:

- If special category data (sensitive information) is accidentally made available via email to unauthorised individuals, the sender must attempt to recall the email as soon as they become aware of the error
- Members of staff who receive personal data sent in error must alert the sender and the DPO as soon as they become aware of the error
- If the sender is unavailable or cannot recall the email for any reason, the DPO will ask Alamo - IT support provider to attempt to recall it from external recipients and remove it from the school's email system (retaining a copy if required as evidence).
- In any cases where the recall is unsuccessful or cannot be confirmed as successful, the DPO will consider whether it is appropriate to contact the relevant unauthorised individuals who received the email, explain that the information was sent in error, and request that those individuals delete the information and do not share, publish, save or replicate it in any way.
- The DPO will endeavor to obtain a written response from all the individuals who received the data, confirming that they have complied with this request.
- The DPO will carry out an internet search to check that the information has not been made public; if it has, we will contact the publisher/website owner or administrator to request that the information is removed from their website and deleted.
- If safeguarding information is compromised, the DPO will inform the designated safeguarding lead.