WFS Personal Data Breach Protocol

Date of last review:	2018	**Review period:**	4 Years
Date of next review:	2022	**Written by:**	Jo Kehoe
Type of policy:	Non-statutory	**Committee:**	Staffing & Resources
Signature:			

Wyre Forest School Personal Data Breach Protocol

This procedure is based on guidance on personal data breaches produced by the ICO.

What is personal data?

Personal data means data which relates to a living individual

What is a personal data breach?

The Data Protection Act 1998 places a legal obligation on organisations to handle personal data securely, in order to avoid that data being put at risk from unauthorised or unlawful processing, accidental loss, destruction or damage.

If an organisation fails to do this and the personal data is put at risk, this may result in a breach of the Act. The following are examples of possible Data Protection breaches/security incidents:

- Personal data being posted to an incorrect address which results in an unintended recipient reading that information;
- Dropping or leaving documents containing personal data in a public place;
- Personal data being left unattended at a printer enabling unauthorised persons to read that information;
- Not storing securely, documents containing personal data (at home or work) when left unattended;
- Any action which allows an unauthorised individual access to Wyre Forest School buildings or computer systems (e.g. through losing a Smart Card, disclosing passwords or writing down passwords etc.);
- verbally disclosing to or discussing personal data with someone not entitled to it, either by phone or in person;
- Deliberately accessing or attempting to access or use personal data beyond the requirements of an individual's job role e.g. for personal, commercial or political use. This action may constitute a criminal offence under the Computer Misuse Act as well as the Data Protection Act.
- Opening a malicious email attachment or clicking on a link from an external or unfamiliar source, which leads to WFS's equipment (and subsequently its records) being subjected to a virus or malicious attack, which results in unauthorised access to, loss, destruction or damage to personal data.

This list is not exhaustive and is provided to illustrate types of data protection breaches.

If you think a breach has taken place

On finding or causing a breach, or potential breach, the staff member or data processor must immediately notify the Data Protection Officer (DPO), if they are not available discuss with another member of SLT. If the breach needs reporting to the ICO, this must happen within 72 hours.

If the breach occurs during a school holiday then the DPO needs to be contacted by phone, if they are not available contact the next member of SLT in the contact list on Appendix 1. SLT will publish their availability during each holiday.

- The DPO will investigate the report and determine whether a breach has occurred and complete a Personal Data Breach Report Form (Appendix 1). 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 unauthorised people
- 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, assisted by relevant staff members or data processors where necessary. (
- The DPO will assess the potential consequences, based on how serious they are, and how likely they are to happen
- The DPO will work out whether the breach must be reported to the ICO. This must be judged on a case-by-case basis. To decide, the DPO will consider whether the breach is likely to negatively affect people's rights and freedoms, and cause them any physical, material or non-material damage (e.g. emotional distress), including through:
    - Loss of control over their data
    - Discrimination
    - Identify theft or fraud
    - Financial loss
    - Unauthorised reversal of pseudonymisation (for example, key-coding)
    - Damage to reputation
    - Loss of confidentiality
    - Any other significant economic or social disadvantage to the individual(s) concerned

  If it's likely that there will be a risk to people's rights and freedoms, the DPO must notify the ICO.
- The DPO will document the decision (either way), in case it is challenged at a later date by the ICO or an individual affected by the breach. Documented decisions are stored within a pass-worded file on the school secure server.
- Where the ICO must be notified, the DPO will do this via the 'report a breach' page of the ICO website within 72 hours. 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. 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
- The DPO will also assess the risk to individuals, again based on the severity and likelihood of potential or actual impact. If the risk is high, the DPO will promptly inform, in writing, all individuals whose personal data has been breached. This notification will set out:
    - 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 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 within a pass-worded file on the school secure server.

  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.

Appendix 1

PERSONAL DATA SECURITY BREACH REPORT FORM

If you discover a personal data security breach, please notify your Head of Department immediately. Please complete this form and return it to the DPO in the first instance, if they are not available to another member of the senior leadership team as soon as possible.

Notification of Data Security Breach	
Date(s) of Breach:	
Date Incident was discovered:	
Name of Person Reporting Incident:	
Contact Details of Person Reporting Incident:	
Brief description of the potential breach:	
Category & number of subjects affected:	
Brief description of any action since the breach was discovered:	
Was the incident reported to the ICO?	

DPO & SLT Contact information

DPO – Jo Kehoe 07725 689362

Headteacher – Rebecca Garratt 07568 301814

Deputy Headteacher – Brian Thomas 07917 333056

Assistant Headteacher – Alison Hopkins 07874 218457

Business Manager – Lyn Cole 07762 700713