Woodlands Primary School

Personal Data Breach Reporting Procedure

Written by	Corinna Taylor
Ratified by Governors	May 2018
Date for Review	May 2021
Signed – Chair of Governors	
Signed – Headteacher	

This policy has been impact assessed by Mark Burns in order to ensure that it does not have an adverse effect on race, gender or disability equality.

To comply with Article 32 of the General Data Protection Regulation (EU) 2016/679 (GDPR) – Security of Processing – Woodlands Primary School has implemented appropriate technical and organisational measures to ensure a level of security appropriate to the risk.

Woodlands Primary School has procedures in place to detect, report and investigate a Personal Data Breach.

To view our procedures on prevention and detection please see Woodlands Primary School Information Security Policy

The GDPR has introduced a general data breach notification at EU level.

Article 33 – Notification of a Personal Data Breach to the Supervisory Authority.

Article 34 – Communication of a Personal Data Breach to the Data Subjects.

What is a Personal Data Breach?

Under **Article 4(12)** of the GDPR 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 transmitted, stored or otherwise processed.

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. A personal data breach can be broadly defined as a security incident that has affected the confidentiality, integrity or availability of personal data.

	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
✓	Loss of availability of personal data

Recital 87 of the GDPR makes clear that when a security incident takes place, we should quickly establish whether a personal data breach has occurred and, if so, promptly take steps to address it, including telling the Information Commissioner's Office (ICO) if required.

Our Legal Obligations

Article 33 (1) states that in the case of a personal data breach, the controller shall without undue delay and, where feasible, not later than 72 hours after having become aware of it, notify the personal data breach to the supervisory authority competent in accordance with Article 55, unless the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons. Where the notification to the supervisory authority is not made within 72 hours, it shall be accompanied by reasons for the delay.

What happens if we fail to notify?

Non-compliance (Article 77-84) constitutes a serious violation and can result in a significant fine. The fine can be combined with the ICO's other corrective powers under Article 58. Non-compliance may also lead to complaints to the ICO, claims for damages, further data loss and loss of reputation.

Exceptions to the Reporting Rule

If the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons we do not need to report it to the ICO.

In the case of reporting a breach to the Data Subjects – we do not need to report the breach to the Data Subjects if

- We have implemented appropriate technical and organisational protection measures, and those measures were applied to the personal data affected by the personal data breach (e.g. encryption).
- We have taken subsequent measures which ensure that the high risk to the rights and freedoms of data subjects is no longer likely to materialise.
- A communication would involve disproportionate effort. (In such a case, a public communication or similar measure is required).

Does the GDPR require us to take any other steps in response to a breach?

We will document all breaches, regardless of whether or not they need to be reported to the ICO - Article 33(5) requires us to document any personal data breaches, comprising the facts relating to the personal data breach, its effects and the remedial action taken. This documentation shall enable the supervisory authority to verify compliance with Article 33.

Documenting our decision-making process is also part of our overall obligation to comply with the accountability principle – Article 5(2).

The Legal Requirement of Woodlands' Data Processors

To comply with Article 33(2) – the processor shall notify Woodlands Primary School without undue delay after becoming aware of a personal data breach. This requirement allows us to take steps to address the breach and meet our breach-reporting obligations.

To comply with Article 28 - these requirements on breach reporting are detailed in the contracts between Woodlands Primary School and our data processors.

RULES, REGULATIONS AND PROCEDURE FOR REPORTING A PERSONAL DATA BREACH TO THE INFORMATION COMMISSIONER'S OFFICE

When a personal data breach has occurred, we will establish the likelihood and severity of the resulting risk to people's rights and freedoms. If it's likely that there will be a risk then we will notify the ICO; if it's unlikely then we won't report it. However, if we decide we don't need to report the breach, we need to justify this decision (Article 33(5)) so we will document it. This documentation shall enable the ICO to verify our compliance.

In assessing risk to rights and freedoms, it's important to focus on the potential negative consequences for individuals. Recital 85 of the GDPR explains that:

"A personal data breach may, if not addressed in an appropriate and timely manner, result in physical, material or non-material damage to natural persons such as loss of control over their personal data or limitation of their rights, discrimination, identity theft or fraud, financial loss, unauthorised reversal of pseudonymisation, damage to reputation, loss of confidentiality of personal data protected by professional secrecy or any other significant economic or social disadvantage to the natural person concerned."

This means that a breach can have a range of adverse effects on individuals, which include emotional distress, and physical and material damage. Some personal data breaches will not lead to risks beyond possible inconvenience to those who need the data to do their job. Other breaches can significantly affect individuals whose personal data has been compromised. Woodlands Primary School will assess this case by case, looking at all relevant factors.

For exceptions – see page 4

Information required to be included in the notification report – See Template A

Under Article 33(3) when reporting a breach, the following information must be included;

- a description of the nature of the personal data breach including, where possible:
    - the categories and approximate number of data subjects concerned; and
    - the categories and approximate number of personal data records concerned;

- the name and contact details of the Headteacher or other contact point where more information can be obtained;
- a description of the likely consequences of the personal data breach; and
- a description of the measures taken, or proposed to be taken by Woodlands, to deal with the personal data breach, including, where appropriate, the measures taken to mitigate any possible adverse effects.

If we don't have all the required information immediately available

The GDPR recognises that it will not always be possible to investigate a breach fully within 72 hours to understand exactly what has happened and what needs to be done to mitigate it. Article 33(4) states that where, and in so far, it is not possible to provide the information at the same time, the information may be provided in phases without undue further delay.

However, we are expected to prioritise the investigation, give it adequate resources, and expedite it urgently. We must still notify the ICO of the breach when we become aware of it, and submit further information as soon as possible. If we know we won't be able to provide full details within 72 hours, we will explain the delay to the ICO and tell them when we expect to submit more information.

Methods of Reporting the Personal Data Breach to the ICO

V Lonie can call the Security Breach Helpline on 0303 123 1113 (open Monday to Friday, 9am to 5pm). A member of staff will record the breach and advise us what to do next.

Or report in writing using the *Personal Data Breach Notification Form* (See Template A) which should be sent to the email address casework@ico.org.uk (with GDPR Personal Data Breach Notification Form in the subject field)

or by post to the

Information Commissioner's Office,
Wycliffe House,
Water Lane,
Wilmslow,
Cheshire SK9 5AF

Or complete an online form via ICO website – will be updated

What happens next?

When the ICO receives the completed Personal Data Breach Notification Form they will contact us within seven calendar days to provide us with

- a case reference number; and
- information about our next steps

If we need any help with the form we can contact the ICO helpline on 0303 123 1113 or 01625 545 745 (operates 9am to 5pm Monday to Friday)

RULES, REGULATIONS AND PROCEDURE FOR REPORTING A PERSONAL DATA BREACH TO THE DATA SUBJECTS

When do we need to tell data subjects about a personal data breach?

When the personal breach is likely to result in a high risk to the rights and freedoms of natural persons, under Article 34(1) Woodlands Primary School shall communicate the personal data breach to the data subject without undue delay.

A 'high risk' means the threshold for informing individuals is higher than for notifying the ICO. Woodlands will 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, we will promptly inform those affected, particularly if there is a need to mitigate an immediate risk of damage to them. Informing individuals helps them take steps to protect themselves from the effects of a breach.

If we decide not to notify individuals, we will still notify the ICO unless we can demonstrate that the breach is unlikely to result in a risk to rights and freedoms. We understand that the ICO has the power to compel us to inform affected individuals if they consider there is a high risk.

For exceptions – see page 4

What information must we provide to data subjects when telling them about a breach? See Template B

Article 34(2) - The communication to the data subject shall describe in clear and plain language the nature of the personal data breach and contain at least the information and measures referred to in Article 33(3)(b)(c)(d) ie.

- the name and contact details of the Headteacher and Data Protection Officer or other contact point where more information can be obtained;
- a description of the likely consequences of the personal data breach; and
- a description of the measures taken, or proposed to be taken, to deal with the personal data breach and including, where appropriate, of the measures taken to mitigate any possible adverse effects.

As with any security incident, we will investigate whether or not the breach was a result of human error or a systemic issue and see how a recurrence can be prevented – whether this is through better processes, further training or other corrective steps.

RULES, REGULATIONS AND PROCEDURE FOR A MEMBER OF STAFF TO REPORT A PERSONAL DATA BREACH TO MANAGEMENT

To comply with the GDPR regulations on the reporting of a Personal Data Breach, Woodlands Primary School has systems in place to detect, report and investigate an incident – See our Information Security Policy, Training Programme and Awareness Campaigns. Personal Data Protection also forms part of our Staff Induction Programme.

1. When a member of staff becomes aware of a personal data breach (as outlined on page 3) he/she will immediately inform V Lonie providing all the necessary information so appropriate steps can be taken to minimise/mitigate the effect on the data subjects.

2. He/she will then complete the relevant sections of Template C – Personal Data Breach Report by a Staff Member (page 12).

   The following information will be included

- Details of the personal data at risk
- Details of when the breach was detected and/or when it occurred;
- Details of how the breach was detected and/or how it occurred;
- The data subjects affected;

The management team will complete their sections of Template C which outlines the decision making process. The following information will be included

- Decision made and reasons why we need to report or not report the breach to the ICO
- Decision made and reasons why we need to report or not report the breach to the data subjects
- Next Steps
- Outcome of the decision

Template A – Form to be completed by Woodlands in the event of a Personal Data Breach

Personal Data Breach Notification Report to ICO		
1	**Organisation Details**	
(a) *	**Name of Organisation**	Woodlands Primary School
(b) *	**Controller's Registration Number**	Supply when required
(c) *	**Contact**	Mrs V Lonie, Headteacher. Headteacher@woodlands.kent.sch.uk 01732 355577 Higham School Lane, Hunt Road, Tonbridge, Kent TN10 4BB
2	**Details of the Personal Data Protection Breach**	
(a) *	Detailed description of the incident	
(b) *	When did the incident happen?	
(c) *	How did the incident happen?	
(d)	Reasons why we have delayed in reporting the incident to the ICO	
(e)	Measures we had in place to prevent an incident of this nature occurring.	
3	**Personal Data at Risk**	
a) *	Details of personal data placed at risk. Specifics of any financial or sensitive personal data that has been affected and details of the extent.	
b) *	Categories and approximate number of individuals affected	
c) *	Categories and approximate number of personal data records concerned	
d) *	Are the affected individuals aware that the incident has occurred?	
e) *	Potential consequences and adverse effects on those individuals	
f) *	Have the affected individuals complained to us about the incident?	
4	**Containment and Recovery**	
(a) *	Have we taken any action to minimise/mitigate the effect on the affected individuals? If so, please provide details.	
(b) *	Has the data placed at risk now been recovered? If so, please provide details of how and when this occurred.	
(c) *	What steps have we taken to prevent a recurrence of this incident?	

5	**Training and Guidance**	
(a)	As the data controller, do we provide our staff with training on the requirements of the GDPR? If so, please provide any extracts relevant to this incident here.	
(b)	Please confirm if training is mandatory for all staff. Had the staff members involved in this incident received training and if so when?	
(c)	As the data controller, do we provide any detailed guidance to staff on the handling of personal data in relation to the incident we are reporting? If so, please provide any extracts relevant to this incident here	
6	**Previous Contact with the ICO**	
(a) *	Have we reported any previous incidents to the ICO in the last two years?	
(b) *	If the answer to the above is "yes" please provide: brief details, the date on which the matter was reported and, where known, the ICO reference number.	
	Miscellaneous	
(a)	Have we informed the Police about this incident? If so, please provide further details and specify the Force concerned.	
(b)	Have we informed any other regulatory bodies about this incident? If so, please provide details.	
(c)	Has there been any media coverage of the incident? If so, please provide details of this.	

(*) denotes mandatory fields. We can let them know if we don't know the answer, or we are waiting on completion of an internal investigation. In the wake of a data protection breach, swift containment and recovery of the situation is vital. Every effort should be taken to minimise the potential impact on affected individuals, and details of the steps taken to achieve this should be included in this form.

Template B – Form to be completed by Woodlands to Report a Personal Data Breach to Data Subjects

Personal Data Breach Notification Report to Data Subjects		
1	**Organisation Details**	
(a)	**Name of Organisation**	Woodlands Primary School
(b)	**Contact**	Mrs V Lonie, Headteacher. Headteacher@woodlands.kent.sch.uk 01732 355577 Hunt Road, Tonbridge, Kent TN10 4BB
2	**Details of the Personal Data Protection Breach**	
(a)	Details of the incident	
(b)	When did the incident happen?	
(c)	How did the incident happen?	
(d)	Measures we had in place to prevent an incident of this nature occurring	
3	**Personal Data at Risk**	
(a)	Details of personal data at risk. Specifics of any financial or sensitive personal data that has been affected and details of the extent	
(b)	Potential consequences and adverse effects of the breach	
4	**Containment and Recovery**	
(d)	Action we have taken to minimise/mitigate the effect on you	
	Steps you need to take now to protect yourself from any effects	
(e)	Have we recovered the data?	
(f)	Steps we have taken to prevent a recurrence of this incident?	
(a)	Who have we informed about this incident? (eg. The Police, ICO).	
(b)	Which regulatory bodies have we informed about this incident?	

Template C – Form to be completed by Staff Member to Record Details of a Personal Data Breach

To be completed after verbally reporting details of the breach to V Lonie

PERSONAL DATA BREACH REPORT BY MEMBER OF STAFF		
1	**Report prepared by**	
2	**Reported to**	
3	**Date of Report**	
4	**Date of the breach**	
5	**Details of the breach**	
6	**When did you become aware of the breach?**	
7	**How did you become aware of the breach?**	
8	**Data Subjects affected by the breach?**	
9	**Are Data Subjects aware of the breach?**	
10	**How did the Data Subjects become aware of the breach?**	
11	**Date you attended Training on Information Security and Data Breach Procedures**	
	To be completed by V Lonie	
12	**Do we need to report this breach to the ICO?**	
13	**If "Yes" – Template A to be completed – Date?**	
14	**If "No"– Give reasons referring to Article 33(1)**	The personal breach is unlikely to result in a risk to the rights and freedoms of natural persons
15	**Do we need to report this breach to the Data Subjects affected?**	
16	**If "Yes" – Template B to be completed-Date?**	
17	**If "No" - Give reasons referring to Article 34(3)(a)(b)(c) for exceptions**	
18	**Next Steps**	Document for our own records and to comply with Article 33 and Accountability Principle 5(2)
19	**If reported – details of the outcome**	