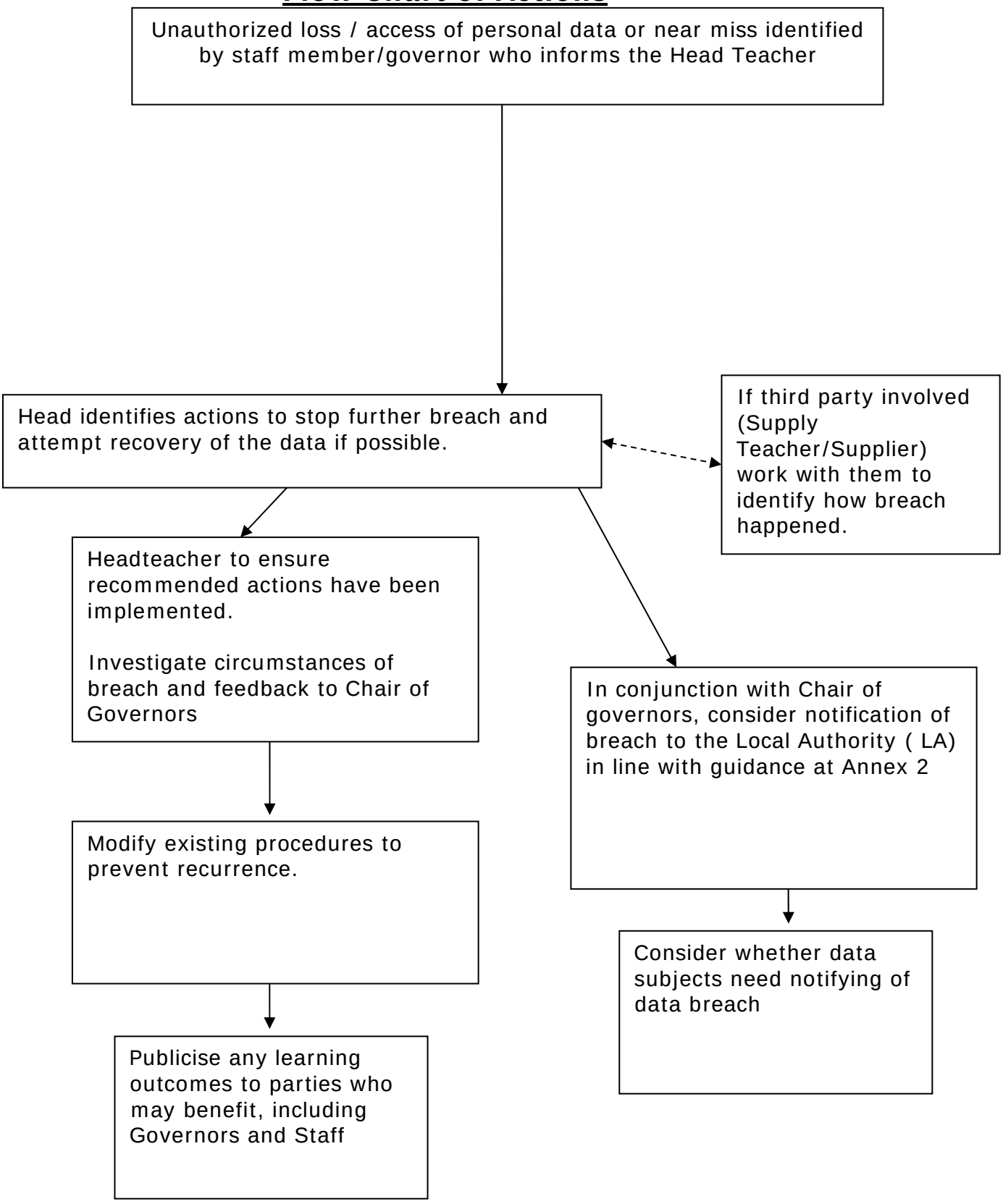
Appendix A to Wyton-on-the-Hill Data Protection Policy	**Incident Plan for Personal Data Breach**

Flow Chart of Actions



1. Definitions

1.1. **Data:** recorded information, whether stored electronically on computer or in paper based filing systems

1.2. **Personal Data**: data (e.g. a name or the postcode of a person's address) which relates to a living individual who can be identified from that data alone or in combination with other information (e.g. Account number and bill). It can be factual or opinion (such as staff Appraisal).

1.3. **Sensitive Data**: Data which relates to Racial or ethnic origin, political opinions, religious or similar beliefs, membership of a Trade Union, physical or mental health or condition, sexual life, commission or alleged commission of an offence, any criminal proceedings. For example sickness records and information on pupils would be sensitive data.

1.4. **Data Subject**: the individual, usually pupil or parent/guardian, who is identified from the personal or sensitive data.

1.5. **Data Breach**: Unofficial and or unnecessary sharing, loss or access to either personal or sensitive data. It includes unauthorised sharing, loss of access to data both within the School and third parties external to the school.

2. PURPOSE OF PROCEDURE

2.1. The purpose of this Plan note is to provide guidance as to what to do in the event of a data breach occurring.

3. SCOPE OF PLAN

3.1. This Plan applies to all near misses or actual data breaches involving the unofficial sharing, loss or access of personal or sensitive data belonging to our pupils, parents/guardians of pupils, staff and governors

3.2. It is to be followed by all staff and governors.

3.3. In the event that a breach happens outside of normal school hours, please notify the Head Teacher or Secretary at the earliest opportunity.

4. STATUS

4.1. School Policy.

5. RESPONSIBILITY

5.1. It is the responsibility of the Head Teacher (as nominated Data Protection Officer –DPO) from time to time to review this Policy and the Privacy Notice which is being used by Wyton School.

6. POLICY

6.1. Why should I follow this plan?

6.2. Breaches of the Data Protection Act 1998 have become an increasingly high profile issue. A breach could damage the school's integrity, reputation and its relationship with its pupils and parents/guardians or expose the pupils, parents/guardians, staff and governors to risks including fraud, identity theft and distress. The school, as a separate entity, could be fined up to £500,000 by the Information Commissioner's Office (ICO) and face criminal prosecution. Individuals may also face prosecution and or disciplinary action.

6.3. What may cause a data breach

6.4. A data breach can be as a result of any of the following (non exhaustive list):

- Loss or theft of data or equipment on which data is stored
- Inappropriate access controls allowing unauthorised and or unnecessary use/ access
- Equipment failure
- Human error
- Unforeseen circumstances such as a fire or flood
- Hacking attack
- 'Blagging' offences where information is obtained by deceiving the organisation who holds it

6.5. Stages in dealing with a data breach

6.6. When a data breach incident occurs, there are four key stages:

i. Containment and recovery of the data.

ii. Assessing the risks to the school and to those whose data has been breached.

iii. Consideration of notification of breaches to persons affected, the ICO and other relevant people within the school (if appropriate once advice has been sought from the DPO).

iv. Evaluation and response

6.7. Immediate Containment and Recovery

6.8. The person who discovers/receives a report of a data breach must inform the DPO. If the breach occurs or is discovered outside normal working hours, this should begin as soon as is practicable.

6.9. The DPO:

- must ascertain whether the data breach is still occurring. If so, steps must be taken immediately to minimise the effect of the breach. An example might be to shut down a system, or to alert relevant staff.
- must inform the Data Protection Officer or Legal Compliance Officer as soon as possible.
- must quickly take appropriate steps to recover any losses and limit the damage. Steps might include:
    i. Inform relevant parties so that they are prepared for any potentially inappropriate enquiries 'phishing' for further information on the incident.
    ii. Contacting recipients of a letter not to open it but destroy/hold/return
    iii. Consideration should be given to a global email if inadvertently sent.

- if an inappropriate enquiry is received by staff/governors, they should attempt to obtain the enquirer's name and contact details and confirm that they will telephone the individual making the enquiry back. Whatever the outcome of the call, it should be reported immediately to the DPO
- consider the use of back-ups to restore lost/damaged/stolen data.
- if the data breach includes any entry codes or passwords, then these codes must be changed immediately, and the relevant agencies and members of staff informed.
- If the breach concerns a breach of Policy then the DPO to be contacted

6.10. Assessing the Risk

6.11. In most cases, the next stage would be for the DPO to fully investigate the breach. The DPO should ascertain whose data was involved in the breach, the potential effect on the data subject(s) and what further steps need to be taken to remedy the situation.

6.12. The investigation, run by the DPO with assistance from the LA if appropriate, should consider the following:

- type of data,
- sensitivity of the data,
- what protections are in place (e.g. encryption),
- what has happened to the data,

- whether the data could be put to any illegal or inappropriate use,
- how many people are affected,
- what type of people have been affected (pupils, parents/guardians etc)
- whether there are wider consequences to the breach.

6.13. The form at Annex 1 must be completed by the DPO member to ensure a clear record is made of the nature of the breach and the actions taken to mitigate it. Once completed it should retained by the DPO be sent to the LA via attachment to an email (with the document password protected due to the sensitive information enclosed). If sent hardcopy please ensure it is in an envelope marked “Private and Confidential”.

6.14. The investigation should be completed urgently and wherever possible within 48 hours of the breach being discovered/reported. A further review of the causes of the breach and recommendations for future improvements can be done once the matter has been resolved.

6.15. Notification

6.16. Some people/agencies may need to be notified as part of the initial containment. However, the decision will normally be made once an investigation has taken place.

6.17. The DPO, will decide whether anyone should be notified of the breach such as the LA, Chair of Governors. In the case of significant breaches, the Information Commissioner’s Office (ICO) may need to be notified. Every incident should be considered on a case by case basis. Annex 2 sets out the relevant considerations.

6.18. Evaluation and Response

6.19. Once the initial aftermath of the breach is over, the DPO should fully review both the causes of the breach and the effectiveness of the response to it. A report may need to be sent to the LA.

6.20. If systemic or ongoing problems are identified, then an action plan must be drawn up to put these right. If the breach warrants a disciplinary investigation, the DPO, leading the investigation, should liaise with the LA for advice and guidance.

6.21. **Annexes**

1. Data Protection Incident Response Evaluation Form
2. Criteria for Notification of the Incident to relevant persons.

ANNEX 1 **CONFIDENTIAL**

Data Protection Incident Response Evaluation Form

Name:……

Date form completed:……..

1. What is the data involved?	
2. How has the data been lost/ shared/ accessed?	
3. How long has the breach been occurring for?	
4. How was the breach discovered?	
5. How many people's data is involved?	
6. Has the data been made available to 'non intended' persons i.e parents/guardians If so, who?	
7. Where is the data now and is it known how many people accessed it? If yes, how many?	
8. How many unauthorised people could have accessed it?	
9. What is being done to recover the data?	
10. Who has been told about the breach?	
11. What policies are in place covering the handling of the data and its security?	
12. What training/awareness raising measures have been taken in the light of this episode?	
13. When did this episode begin?	
14. Has this happened before?	

ANNEX 2

CONSIDERATIONS FOR DECIDING WHO TO NOTIFY

- Potential detriment to data subjects
- The volume of personal data lost / released / corrupted
- The sensitivity of the data involved

Glossary

DPO: Data Protection Officer (Currently the Head Teacher)

ICO: Information Commissioners Office. Responsible for enforcement of the Data Protection Act 1998.