DATA BREACH REPORT FORM

Completed forms must be sent as soon as possible to Jackie Lloyd, Admin Officer. Provide as much information as you can, but do not delay sending in the form, incidents must be notified within 24 hours of identification.

GENERAL DETAILS	
Incident number:	*To be assigned by data protection lead*
Reported by:	*Named member of staff/member of public/parent/carer*
Date of incident:	*When did it occur*
Date incident was identified:	*When was it identified*
Reported Date:	*Date DPO/DP Lead/Head Notified*
Location of incident :	*In school, offsite etc*

ABOUT THE INCIDENT – provide as much information as possible.	
Incident description. Please describe the incident in as much detail as possible	
How did the incident occur?	*Provide as much known information as possible*
When did the incident happen?	*If no accurate date can be identified, be approximate*
How was the incident identified?	*Was it discovered by the school, reported by a parent/3rd party*
What personal data has been placed at risk?	*Details of information you believe may have been*
In what format was the information involved?	*Letter, email, USB pen etc.*
Was the data encrypted/appropriately secured?	*Was secure email used, was USB secure, if system access what controls were in place*

DATA BREACH REPORT FORM

Dealing with the current incident	
Has the school taken any immediate action to minimise/mitigate the effect on the affected individuals?	*If so, provide details.*
How many individuals have been affected?	*Number of pupils, staff, parents etc. who may have been affected by information being put at risk*
Have any affected individuals complained to the school about the incident?	*Have they complained direct, have they referenced complaining to the ICO?*
What are the potential consequences and adverse effects on those individuals? (parents, pupils or staff)	*Don't just think worst case scenario, think of any consequences to individuals even if it is merely 'inconvenience'*
Has the data subject been informed/is the data subject aware?	*Have they already been told or are they likely to be aware e.g. parents talking to each other, was it reported in the press etc.*
Has the data placed at risk now been recovered? If so, please provide details of how and when this occurred.	*Can you verify the risk has been removed – the data recovered or destroyed, vulnerabilities addressed etc.*
Preventing a recurrence	
Has any action been taken to prevent recurrence?	*What steps have been taken – policies, procedures, change in working practice, training etc.*
Are further actions planned? If so, what?	*Have other actions been scheduled, e.g. an audit of processes, training etc.*
Who has the action been agreed by?	*Has any action been signed off by Head, Governors, DPO etc.*
Individuals Involved	
Have the staff involved in the security incident done any Data Protection Training?	*Document what training was carried out*
If so, what and when? (Please list)	*Document when any/last training was carried out*
How long have those involved worked at the School?	*Addresses whether training is required for new staff*

DATA BREACH REPORT FORM

Are the staff involved: agency staff, new starters, part time staff, full time staff etc?	*Addresses whether training is required for different levels of staff, governors etc.*

	IMPACT ASSESSMENT QUESTIONS	
1.	**Was any data lost or compromised in the incident?** E.g. Loss of an encrypted item should not actually have compromised any information.	Yes/No
2.	**Was personal data lost or compromised?** This is data about living individuals such as pupil, staff, parents etc.	Yes/No
3.	**If yes, was <u>sensitive</u> personal data compromised?** This is data relating to health, ethnicity, sexual life, trade union membership, political or religious beliefs, philosophical beliefs, potential or actual criminal offences, genetic or biometric data.	Yes/No
4.	**Does any of the information lost or compromised relate directly to a child/children?**	Yes/No
5.	**Was safeguarding, child protection or health data involved?**	Yes/No
6.	**What is the number of people whose data was affected by the incident?**	
7.	**Is the data breach <u>unlikely</u> to result in a <u>risk</u> to the individual/individuals? Physically, materially, or morally?** Example - physical harm, fraud, reputation, financial loss, distress	Yes/No
8.	**Did this incident involve information belonging to another organisation?** e.g. NHS, Local Council, Police etc.	Yes/ No
9.	**Did people affected by the incident give the information to the School in confidence?** (i.e. with an expectation that it would be kept confidential)	Yes/No
10.	**Is there a risk that the incident could lead to direct damage to any individual** e.g. via identity theft/ fraud/impersonation?	Yes/No
11.	**Could the incident damage an individual's reputation, or cause hurt, distress, embarrassment or humiliation** e.g. loss of medical records, disciplinary records etc.?	Yes/No
12.	**Can the incident have a serious impact on the School's reputation?**	Yes/No
13.	**Has any similar incident happened before?**	Yes/No
14.	**Was the school aware such an incident was possible or likely to occur?**	Yes/No

DATA BREACH REPORT FORM

REVIEW: to be completed by Data Protection Lead/Data Protection Officer (where required)	
Incident Number:	
Classification:	[ ] Breach [ ] Incident [ ] Offence
Principles identified as breached:	1) Lawful, fair and transparent
	2) Specific, explicit and legitimate purposes
	3) Adequate, relevant and limited to what is necessary for processing.
	4) Accurate and kept up to date
	5) Kept in a form that allows for the identification of data subjects only as long as necessary
	6) Processed in manner that ensures its security.

Is a full investigation required?	
Have data subjects been informed?	
Have key stakeholders (Parents, Governors, Local Authority etc) been informed?	
Have control weaknesses been highlighted and recommendations made?	
Has sufficient and appropriate action been taken?	
Does the incident need reporting to the DPO?	
Does the incident need reporting to the ICO?	
Has the Incident Log been updated?	
Further investigation undertaken by:-	
Notes: **(Reasons for referral/non-referral to**	

DATA BREACH REPORT FORM

ICO)	

Sign off and Outcomes		
Item	**Name/Date**	**Notes**
Measures to be implemented approved by:		*Responsibility for actions and required completion date – school DP Lead/Head*
DPO advice and recommendation provided:		*DPO advice in relation to mitigating risk, action to be taken*
Summary of DPO Advice:		
DPO Advice accepted or overruled by:		*If overruled, reason must be stated and by whom*
Comments:		
Date Closed:		