SPARKEN HILL
ACADEMY

UK GDPR
Data Breach Plan (Inc Monitoring & Report)

Rev	Date Is-sued	Prepared By	Approved	Review Date	Com-ments
1.2	Feb 2021	RTL	Feb 2022	Feb 2023	
	Feb 2022	RTL	Feb 2023	Feb 2024	
	Feb 2023	RTL	Feb 2024	Feb 2025	
	Feb 2024	RTL	Feb 2025	Feb 2026	

Data breach monitoring record

1 General information

Date of monitoring review	[*insert date of monitoring review*]
Person conducting monitoring review	[*insert name*]

1.1 Volume of data breaches identified and reported

Review your data breach register for the past 12 months and complete the information below.

Category	Over the last 12 months
Suspected data security breaches	[*insert number of suspected data security breaches over the period*]
Actual data security breaches	[*insert number of actual data security breaches*]
Reports to the ICO (involving actual or suspected data security breaches)	[*insert number of reports sent to the ICO*]
Data subjects notified of actual or suspected data security breaches	[*insert number of data subjects notified of suspected data security breaches*]
Reports to the police (involving actual or suspected data security breaches)	[*insert number of reports sent to the police*]
Insurer notifications (involving actual or suspected data security breaches)	**[**Cyber insurance notifications: [*insert number*]**]** **[**Crime insurance notifications: [*insert number*]**]**

1.2 Causes of data breaches

Consider the root cause of any actual or suspected data breaches. This will help to identify trends and risk areas.

Cause of breach	Over the last 12 months
Loss or theft of paperwork	[*insert number of incidents involving loss or theft of paperwork*]
Data posted or faxed to incorrect recipient	[*insert number of times data has been posted or faced to an incorrect recipient*]
Data sent by email to incorrect recipient	[*insert number of times data has been sent by email to an incorrect recipient*]
Insecure web page (including hacking)	[*insert number of instances of web page insecurity*]
Failure to redact data	[*insert number of times data has not been appropriately redacted*]
Insecure disposal of paperwork	[*insert number of times in which paperwork has not been disposed of securely*]
Loss or theft of unencrypted device	[*insert number of times unencrypted devices have been lost or stolen*]
Secure information uploaded to web page	[*insert number of times secure information has been uploaded to a webpage*]
Verbal disclosure of special categories of personal data	[*insert number of times special categories of personal data have been disclosed verbally*]
Insecure disposal of hardware	[*insert number of times hardware has not been disposed of securely*]

Cause of breach	Over the last 12 months
Other (please state)	[*insert number*]

1.3 **Review and findings**

Is the data breach register up to date?	Yes/No
Have you identified any new data breaches as a result of this review ?	Yes/No
If yes: what is the nature of the breach? has the breach been reported to the police or ICO? has the breach been notified to any relevant insurer? has the breach been notified to relevant data subjects? has the breach been recorded in the data breach register?	[*insert responses*]
Has this review identified any training needs within Sparken Hill Academy Trust?	Yes/No
If yes, give details	[*insert any training needs within Sparken Hill Academy Trust Is this new or refresher training refresher?*]
Do we need to take any remedial, preventative or other action as a result of this review?	[*Insert*]
If yes, give details	[*Insert, eg draft a new policy or update an existing policy/procedure*]

Data breach report form

If you know or suspect a data security breach has occurred, please:

complete this form, and
email or deliver it to the Business Manager or Data Protection Officer at dpo@sparkenhill.com
ensuring you mark your email or the form as urgent

Name and contact details of person notifying the actual or suspected breach	[*Insert name and contact details*] *If you wish to submit an anonymous report, leave this section blank.*
Dept/manager	[*Insert department from which the report emanated and the relevant manager*]
Date of actual or suspected breach	[*Insert date*]
Date of discovery of actual or suspected breach	[*Insert date*]
Date of this report	[*Insert date*]
Summary of the facts	[*Provide as much information as possible—including the amount, sensitivity and type of data involved*]
Cause of the actual or suspected breach	[*Provide a detailed account of what happened*]
Is the actual or suspected breach ongoing?	**[**Yes OR No**]**
Who is or could be affected by the actual or suspected breach?	[*Include details of categories and approximate number of data subjects concerned*] *Do not notify affected data subjects. The data breach team will determine who should be notified and how.*
Are you aware of any related or other data breaches?	**[**Yes OR No**]** [*If yes, provide more details*]

Data breach plan

1 **Introduction**

1.3.1

1.3.2 This data protection breach plan:

1.4 places obligations on staff to report actual or suspected breaches of personal data security, and

1.5 sets out our procedure for managing and recording actual or suspected breaches

1.5.1

1.5.2 This plan applies to all staff and to all personal data and special categories of personal data held by Sparken hill Academy Trust. This plan supplements our policies relating to data protection.

1.6 For the purpose of this plan:

Data breach team means the team responsible for investigating data security breaches. This team can include members of the Senior Leadership Team, Learning Technologies Manager, Information Technologies (IT) consultant and the Data Protection Officer DPO

Data security breach

1.5.1 Means '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;

1.5.1 **Information Commissioner's Office (ICO)**

1.5.1 means the UK's independent data protection and information regulator.

1.5.1

1.5.1 **Personal data**

1.5.1 means any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person;

1.5.1

1.5.1 **Special categories of personal data**

1.7 Means personal data about an individual's racial or ethnic origin, political opinions, religious or similar beliefs, trade union membership (or non-membership), physical or mental health or condition, sex life or sexual orientation, genetic or biometric data.

1.5.1

1.1 **Responsibility**

The Principal, Richard Lilley has overall responsibility for this plan. They are responsible for ensuring it is adhered to by all staff.

1.2 **Our duties**

1.3.1

Sparken Hill Academy Trust processes personal data relating to individuals including staff, clients and third parties. As custodians of data, we have a responsibility under the General Data Protection Regulation (GDPR) to protect the security of the personal data we hold.

2 We must keep personal data secure against loss or misuse. All staff are required to comply with our security guidelines and policies.

1.3 **What can cause a data security breach?**

1.3.1

1.5.1 A data security breach can happen for a number of reasons:

2.1 loss or theft of data or equipment on which data is stored, eg loss of a laptop or a paper file

2.2 Inappropriate access controls allowing unauthorised use

2.3 Equipment failure

2.4 Human error, eg sending an email to the wrong recipient

2.4.1 Unforeseen circumstances such as a fire or flood

2.4.2 Hacking, phishing and other 'blagging' attacks where information is obtained by deceiving whoever holds it

2.5 **If you discover a breach**

1.3.1

2.6 If you know or suspect a data security breach has occurred or may occur, you should:

3 Complete a data breach report form, which can be located at the main office, on the staff board by the Riso machine or on the academy network.

3 The form asks for your name, but you do not have to give it if you would prefer to report the failure anonymously

3.1 Email the completed form to dpo@sparkenhill.com

3.1 If you wish to make an anonymous report, you can submit the form by a non-electronic method, eg internal post to the Principal or Business Manager.

1.5.1

3.2 Where appropriate, you should liaise with your line manager about completion of the report form. However, this may not be appropriate or possible, eg if your line manager is aware of the breach and has instructed you not to report

it, or if they are simply not available. In these circumstances, you should submit the report directly to the Principal or Business Manager without consulting your line manager.

4 You should not take any further action in relation to the breach. In particular, you must not notify any affected individuals or regulators. The Principal, Business Manager or DPO will acknowledge receipt of the report form (if the person making the report has given their name) and take appropriate steps to deal with the report in collaboration with the data breach team.

4.1 **Managing and recording the breach**

1.3.1

4.1.1 On being notified of a suspected data security breach, the *DPO* will establish a OR assemble the data breach team—see Appendix 2. The data breach team will be led by DPO*.*

4.1.2 The data breach team will take immediate steps to establish whether a breach has, in fact, occurred. If so, the data breach team will take appropriate action to:

Contain the data breach and (so far as reasonably practicable) recover, rectify or delete the data that has been lost, damaged or disclosed

6.2.2 Assess and record the breach in Sparken Hill Academy Trust data security breach register

4.1.4 Notify appropriate parties of the breach

6.2.4 Take steps to prevent future breaches

4.3 These are explained below.

1.5.1

5 **Containment and recovery**

6 The data breach team will identify how the security breach occurred and take immediate steps to stop or minimise further loss, destruction or unauthorised disclosure of data

6.1 The data breach team will identify ways to recover, correct or delete data. This may include contacting the police, eg where the breach involves stolen hardware or data

6.1.1 Depending on the nature of the breach, the data breach team will notify Sparken Hill Academy Trust Risk Protection Department through the Department for Education (DFE) as the insurer can provide access to data breach management experts.

6.1.1

6.1.2 **Assess and record the breach**

6.1.3 Having dealt with containment and recovery (see paragraph 6.3), the data breach team will assess the risks associated with the breach, including:

6.1.4

6.1.5 What type of data is involved?

6.1.6 How sensitive is the data?

(c) Who is affected by the breach, ie the categories and approximate number of data subjects involved?

6.3 The likely consequences of the breach on affected data subjects, eg what harm can come to those individuals, are there risks to physical safety or reputation, or financial loss?

6.3.1 Where data has been lost or stolen, are there any protections in place such as encryption?

6.3.2 What has happened to the data, eg if data has been stolen, could it be used for harmful purposes?

7 What could the data tell a third party about the data subject, eg could the loss of apparently trivial snippets of information help a determined fraudster build up a detailed picture of other people?

7.1 What are the likely consequences of the personal data breach on Sparken Hill Academy Trust, eg loss of reputation, loss of business, liability for fines?

7.2 Are there wider consequences to consider, eg loss of public confidence in an important service we provide?

4.3

7.2.1 This information should be recorded in Sparken Hill Academy Trust's data breach register

1.5.1

6.5 **Notifying appropriate parties of the breach**

7.2.3 The data breach team will consider whether to notify:

6.1.4

6.1.5 Affected data subjects

6.1.6 The police

(c) The ICO

6.3.1 Any other parties, eg insurers or commercial partners

4.3

7.2.4 **Notifying data subjects**

4.3 In determining whether to notify affected data subjects, the data breach team will have regard to whether there is a high risk to the data subjects. The team will consider who should be notified, how and what they should be told, taking into account the following factors:

6.1.5 Can notification help the individual(s), eg could individuals act on the information to mitigate risks by cancelling a credit card or changing a password?

6.1.6 Will notification mitigate the harm done to an individual or pointlessly alarm them in circumstances where they can do nothing with that information?

(c) Are there any legal or contractual requirements to notify the data subject?

6.3 Is there a danger of over-notifying—not every incident will warrant notification and notifying the entire customer-base of an issue affecting only a small percentage of clients may well cause disproportionate enquiries and work?

6.3.1 What is the best way of notifying affected individuals, taking into account the security of the notification method and the urgency of the situation?

6.3.2 Do any individuals or categories of individuals need to be treated with special care, eg if the breach involves data relating to children or vulnerable adults?

7 What information should be provided to individuals about the steps they can take to protect themselves and what we can do to help them?

7.1 How should affected individuals contact us for further information or to ask questions—this could be a helpline number or a web page?

7.2 Will notification help Sparken Hill Academy Trust meet its security obligations?

4.3

7.3 **Notifying the police**

4.3 The data breach team will already have considered whether to contact the police for the purpose of containment and recovery (see paragraph 6.3). Regardless of this, if it subsequently transpires that the breach arose from a criminal act perpetrated against, or by a representative of**,** Sparken Hill academy Trust, the data breach team will notify the police and/or relevant law enforcement authorities.

6.5.4 **Notifying the ICO**

4.3 The data breach team will notify the ICO when there is a risk to the data subjects. If the data breach team is unsure whether or not to report, the presumption should be to report. The data breach team will take account of relevant ICO guidance, summarised below:

The potential harm to data subjects

This is the overriding consideration in deciding whether a breach of data security should be reported to the ICO. Detriments include emotional distress as well as both physical and financial damage. It can include:

—exposure to identity theft through the release of non-public identifiers, eg passport number

—information about the private aspects of a person's life becoming known to others, eg financial circumstances

Significant actual or potential detriment should be reported, whether because of the volume of data, its sensitivity or a combination of the two.

There is no need to report where there is little risk that individuals would suffer significant detriment, eg because a stolen laptop is properly encrypted or the information is publicly-available.

The volume of personal data

There should be a presumption to report to the ICO where:

—a large volume of personal data is concerned, and

—there is a real risk of individuals suffering some harm

It will, however, be appropriate to report much lower volumes in some circumstances where the risk is particularly high, eg because of the circumstances of the loss or the extent of information about each individual.

The ICO provides two examples:

—loss of an unencrypted laptop holding names, addresses, dates of birth and National Insurance numbers of 100 individuals would be reportable

—loss of a marketing list of 100 names and addresses (or other contact details) where there is no particular sensitivity of the service being marketed would not be reportable

The special categories of data

There should be a presumption to report to the ICO where smaller amounts of personal data are involved, the release of which could cause a significant risk of individuals suffering substantial detriment, including substantial distress.
This is most likely to be the case where the breach involves special categories of personal data. If the information is particularly sensitive, even a single record could trigger a report.
The ICO provides two examples:
—theft of a manual paper-based filing system (or unencrypted digital media) holding the personal data and financial records of 50 named individuals would be reportable
—breach of a similar system holding the trade union subscription records of the same number of individuals (where there are no special circumstances surrounding the loss) would not be reportable

6.5.5 **Notifying other parties**

4.3 The data breach team will consider whether there are any legal or contractual requirements to notify any other parties.

4.3 The data breach team will:

6.6.1 Establish what security measures were in place when the breach occurred

6.6.2 Assess whether technical or organisational measures can be implemented to prevent the breach happening again

6.6.3 Consider whether there is adequate staff awareness of security issues and look to fill any gaps through training or tailored advice

9 Consider whether it is necessary to update Sparken Hill Academy Trust privacy risk assessment

6.6.5 Update Sparken Hill Academy Trust's privacy risk register

6.6.6 Debrief data breach team members following the investigation

7 Monitoring and review

7.1 We will monitor the effectiveness of all our policies and procedures regularly, and conduct a full review and update as appropriate, at least annually.

7.2 Our monitoring and review exercises will include looking at how our policies and procedures are working in practice to reduce the risks posed to our company.

8 Staff awareness and training

8.1 Key to the success of our systems is staff awareness and understanding.

8.2 We provide regular training to staff:

- 8.2.1 At induction
- 8.2.2 When there is any change to the law, regulation or our policy
- 8.2.3 At least annually
- 8.2.4 When significant new threats are identified
- 8.2.5 In the event of an incident affecting our company or a competitor

9 Reporting concerns

Prevention is always better than cure. Data security concerns may arise at any time and we encourage you to report any concerns you have to the Principal, Business Manager or DPO. This helps us capture risks as they emerge, protect our company from data security breaches, and keep our processes up-to-date and effective.

10 Consequences of non-compliance

10.1 Failure to comply with this plan and associated data protection policies puts you and Sparken Hill Academy Trust at risk. Failure to notify the Principal, Business Manager or DPO of an actual or suspected data security breach is a very serious issue.

10.2 You may be liable to disciplinary action if you fail to comply with the provisions of this, and all related plans, policies and procedures.

Appendix 1

Data breach report form

Appendix 2

Data Breach Team

Data breach team lead - DPO	The DP Advice Service Ltd
Principal	Richard Lilley
Learning Technologies Manager	Chris Johnson
Vice Principal	Kate Phoenix
Assistant Principal	Laura Grayson
Assistant Principal	Helen Brentnall
Assistant Principal	Victoria Marshall
Senior Family Support Officer	Karen Gardiner
Teaching Assistant Manager	Jeremy Cordall
Information Technologies Consultant (IT)	Adam Ross

Data breach assessment and action plan

1 Data breach team

Guidance: the first step is to assemble a team to manage and respond to the breach.

Data breach team lead	[*Insert the name or description of the person who will lead the data breach team, eg DPO*]
Head of legal	[*Insert name*]
Head of compliance	[*insert name*]
Head of IT	[*Insert name*]
[*Insert any other, eg Head of HR if the breach involves employee data*]	[*Insert name*]

1.1 Background information

Guidance: refer to the data breach report form, if appropriate.

Name of person notifying the actual or suspected breach	[*Insert name*]
Dept and manager	[*Insert department from which the report emanates and manager for that department*]
Date of actual or suspected breach	[*Insert date*]
Date of discovery of actual or suspected breach	[*Insert date*]
Date actual or suspected breach notified internally	[*Insert date*]

1.2 Preliminary assessment

Guidance: as soon as possible you should take steps to contain the breach and recover lost data, but before you can do this you will need to make a preliminary assessment of what data has been lost, why and how.

Summary of the facts	[*Provide as much information as possible—including the amount, sensitivity and type of data involved*]
Categories and approximate number of data subjects concerned	[*Insert details of categories and approximate number of data subjects concerned*]
Categories and approximate number of personal data records concerned	[*Insert details of categories and approximate number of personal data records concerned*]
How sensitive is the data?	[*Insert details*]
Cause of the actual or suspected breach	[*Insert details*]
Any other comments	[*Insert comments*]

1.3 Containment and recovery

Guidance: having assembled your data breach team and undertaken a preliminary assessment, containment and recovery should be your first priority. You should consider notifying any relevant insurer, eg your cyber, professional indemnity or crime insurer. The insurer/broker can usually provide access to data breach management experts and cyber insurance usually covers breach response costs.

Does SPARKEN HILL ACADEMY TRUST Ltd have cyber insurance?	Yes/No *If yes, notify the insurer immediately as they can provide access to experts in data breach management,*

	and the policy is likely to cover breach response costs.
Is the actual or suspected breach ongoing?	Yes/No
What steps can be taken to stop or minimise further loss, destruction or unauthorised disclosure of data?	[*Insert comments, eg if a mobile device is lost can it be wiped remotely?*]
What immediate steps can be taken to recover, correct or delete data?	[*Insert comments*]
Should the breach be reported to the police, eg is there evidence of theft?	[*Insert comments*]
Does Sparken Hill Academy Trust have crime insurance?	Yes/No *If yes (and the breach arises out of a criminal event), notify the insurer immediately. The insurer/broker can usually provide access to data breach management experts, though the policy is unlikely to cover breach response costs.*
Does Sparken Hill Academy Trust have any other relevant insurance, eg professional indemnity?	Yes/No *If yes, notify your insurer. The insurer/broker can usually provide access to data breach management experts, though the policy is unlikely to cover breach response costs.*
Any other comments	[*Insert comments*]

2.5 **Detailed assessment and record keeping**

Guidance note: once you have taken steps to contain and recover the data, you should undertake a full assessment and record the breach in a central register.

What type of data is involved?	[*Insert description of data involved*]
How sensitive is the data?	*[Insert, ie does the breach involve special categories of personal data?]*
Who is affected by the breach?	[*State the categories and approximate number of data subjects involved*]
What are the likely consequences of the breach on affected data subjects?	[*Insert, eg what harm can come to those individuals, are there risks to physical safety or reputation or financial loss?*]
Where data has been lost or stolen, are there any protections in place such as encryption?	[*Insert details of protections in place*]
What has happened to the data?	[*Insert, eg if data has been stolen, could it be used for harmful purposes?*]
What could the data tell a third party about the data subject?	[*Insert, eg could the loss of apparently trivial snippets of information help a determined fraudster build up a detailed picture of other people?*]

Are there any related or other data breaches?	Yes/No [*If yes, provide more details*]
Is there a pattern or trend of similar breaches?	Yes/No [*If yes, provide more details*]
Have you recorded the breach in the organisation's Data breach register?	[*Yes/No*] *If no, why not?*
Are there wider consequences to consider?	[*Insert, eg loss of public confidence in an important service you provide*]
Any other comments	[*Insert comments*]

4.1 **Notifying data subjects**

In determining whether to notify affected data subjects, you should have regard to ICO regulatory guidance that notification should have a clear purpose, eg to warn individuals to take protective action. This is reflected in the table below.

Can notification help the individual(s)?	[*Insert, eg could individuals act on the information to mitigate risks by cancelling a credit card or changing a password*]
Is there any legal or contractual requirement to notify the data subject?	[*Insert, eg in your customer retainer or under a referral agreement*]
Is there a danger of over-notifying? *Guidance: not every incident will warrant notification and notifying your entire customer-base of an issue affecting only a small percentage of customers may well cause disproportionate enquiries and work.*	[*Insert possible dangers of over-notifying, if applicable*]
What is the best way to notify affected individuals?	[*Insert, taking into account the security of the notification method and the urgency of the situation*]
Do any individuals or categories of individuals need to be treated with special care?	[*Insert, eg if the breach involves children or vulnerable adults*]
What information should be provided to individuals about the steps they can take to protect themselves and what we can do to help them?	[*Insert information to provide to individuals*]
How should affected individuals contact Sparken Hill Academy Trust for further information or to ask questions?	[*Insert methds of contact, eg this could be a helpline number or a web page*]
Will notification help Sparken Hill Academy Trust meet its security obligations?	[*Insert comments*]
Taking the above factors into account, should affected data subjects be notified?	Yes/No *If no, state your reasons, if yes, see below*

If yes to the above question: [*Insert answers to each question*]

—which data subjects should be notified?
—how should data subjects be notified)
—what information will be provided?
—how will Sparken Hill Academy Trust manage responses or request further information?
—how will Sparken Hill Academy Trust track who has been notified?
Any other comments [*Insert comments*]

7 Notifying the ICO

You should notify the ICO when a serious breach has occurred. If you are unsure whether or not to report, the presumption should be in favour of reporting. Consider the factors below and in Sparken Hill Academy Trust's data breach plan.

Factor 1: potential harm to data subjects

[*Insert your conclusions on the potential harm to data subjects*]
Guidance: this is the overriding consideration in deciding whether a breach of data security should be reported to the ICO. Detriments include emotional distress as well as both physical and financial damage. It can include:
—exposure to identity theft through the release of non-public identifiers, eg passport number
—information about the private aspects of a person's life becoming known to others, eg financial circumstances
Significant actual or potential detriment should be reported, whether because of the volume of data, its sensitivity or a combination of the two.
There is no need to report where there is little risk that individuals would suffer significant detriment, eg because a stolen laptop is properly encrypted, or the information is publicly-available.

Factor 2: volume of personal data involved in the breach
[*Insert your conclusions on the volume of data involved*]
Guidance: there should be a presumption to report to the ICO where:
—a large volume of personal data is concerned and
—there is a real risk of individuals suffering some harm
It will, however, be appropriate to report much lower volumes in some circumstances where the risk is particularly high, eg because of the circumstances of the loss or the extent of information about each individual.

Factor 3: sensitivity of data
[*Insert your conclusions on the sensitivity of data involved*]
Guidance: there should be a presumption to report to the ICO where smaller amounts of personal data are involved, the release of which could cause a significant risk of individuals suffering substantial detriment, including substantial distress.
This is most likely to be the case where the breach involves special categories of personal data. If the information is particularly sensitive, even a single record could trigger a report.
Decision
Taking the above factors into account, we will **[**not**]** notify the ICO

8 Notifying others

Guidance note: consider whether to notify others, eg the police, any professional regulator or business partners.

Is it necessary to notify the police and/or any other relevant law enforcement authority? *Guidance: you should already have considered this issue for the purpose of containment and recovery (see section 4). Nevertheless, further information may now be available and you should consider this issue again.*	Yes/No [*If the breach involves criminal activities but you have decided not to notify the police, state your reasons*]
It is necessary to notify any professional regulator or trade body?	Yes/No
Is there any legal or contractual requirement to notify any other parties, eg pursuant to an outsourcing contract?	Yes/No [*If yes, give further information*]
Any other comments	[*Insert comments*]

9 Preventing future breaches

Guidance note: you should evaluate your response to the breach and implement the changes necessary to prevent a recurrence.

What security measures were in place when the breach occurred?	[*Insert details*]
What technical organisational measures could be implemented to prevent the breach happening again?	[*Insert, eg ensure remote devices are properly encrypted and can be wiped remotely*]
Is there adequate staff awareness of security issues? Are there any gaps to fill through training or tailored advice?	[*Insert details of staff awareness and training required*]
Is it necessary to **[**conduct a OR update Sparken Hill Academy Trust's**]** privacy risk assessment?	[*Insert details of the action needed*]
Is it necessary to update Sparken Hill Academy Trust 's privacy risk register?	[*Insert details of updates required, if any*]
Any other comments	[*Insert comments*]

Data breach—panic sheet

1. Data breach team

Damage limitation is a priority immediately following a security breach. You will need a team of people to manage the data breach.

Actions

Assemble a data breach team, including your Data Protection Officer (DPO) (if you have one), head of legal/compliance, head of IT and head of HR (if employee data is involved).
Appoint someone to lead the team (preferably not your head of IT).

2. Preliminary notifications

Your first instinct may be to tell affected individuals and regulators about the breach, but you need more information before you can decide whether this is necessary or desirable. Your focus during the first 24 hours should be on containment and recovery.

Recommendation

Unless there are compelling reasons, do not at this stage notify:

affected data subject(s)
the Information Commissioner's Office (ICO)

3. Preliminary assessment

You should take steps to contain the breach and recover lost data as soon as possible, but before you can do this you will need to do a preliminary assessment of what data has been lost, why and how.

Actions

Conduct a preliminary assessment, using Precedent: Data breach assessment and action plan.

4. Containment and recovery

Having assembled your data breach team and undertaken a preliminary assessment, containment and recovery should be your priority.

External experts can help you respond to a data security breach. Unless you've identified data breach management experts in advance, you'll need guidance on whether to get external help and, if so, from whom. Your insurer or broker should be able to put you in touch with tried and tested experts. Depending on the type of insurance you have, your insurer may well have a vested interest in mitigating the damage and/or associated costs, plus your insurance may cover breach response costs.

Actions

Check whether you have cyber insurance—if yes, call your broker or insurer immediately. The insurer will provide access to data breach management experts and your policy should cover breach response costs.
If the breach arises out of a criminal event:

- check whether you have crime insurance. If yes, call your crime insurer immediately. The insurer or broker can usually recommend data breach management experts, though your policy is unlikely to cover breach response costs
- notify the police

If relevant, consider calling your professional indemnity insurer, especially if the breach involves third party data, e.g. customer data. Even if the breach doesn't involve third party data, your broker should be able to recommend data breach management experts (your policy is unlikely to cover breach response costs).

Work with your internal and external experts to:

- prevent or minimise further loss, destruction or unauthorised disclosure of data
- recover, correct or delete lost, corrupted or stolen data

5. Subsequent actions

If possible, you should complete the above actions on the day the data breach is recovered and, if that is not possible, within the first 24 hours.

This is not, however, the end of the matter. Having dealt with the immediate aftermath of the data breach, you will then need to:

undertake a full assessment and record the breach in a central register
consider whether to notify affected data subjects
consider whether to notify the ICO
consider whether to notify anyone else, e.g. a business party pursuant to a contractual obligation
evaluate your response to the breach and implement the changes necessary to prevent a recurrence

See sections 5 to 9 of Data breach assessment and action plan.